TIA DOCUMENT

IP Over Satellite (IPoS)

TIA-1008

OCTOBER 2003

TELECOMMUNICATIONS INDUSTRY ASSOCIATION

The Telecommunications Industry Association represents the communications sector of

Electronic Industries Alliance

NOTICE

TIA Engineering Standards and Publications are designed to serve the public interest through eliminating misunderstandings between manufacturers and purchasers, facilitating interchangeability and improvement of products, and assisting the purchaser in selecting and obtaining with minimum delay the proper product for their particular need. The existence of such Publications shall not in any respect preclude any member or non-member of TIA from manufacturing or selling products not conforming to such Publications. Neither shall the existence of such Documents preclude their voluntary use by non-TIA members, either domestically or internationally.

TIA DOCUMENTS

TIA Documents contain information deemed to be of technical value to the industry, and are published at the request of the originating Committee without necessarily following the rigorous public review and resolution of comments which is a procedural part of the development of a American National Standard (ANS). Further details of the development process are available in the TIA Engineering Manual, located at http://www.tiaonline.org/standards/sfg/engineering_manual.cfm

TIA Documents shall be reviewed on a five year cycle by the formulating Committee and a decision made on whether to reaffirm, revise, withdraw, or proceed to develop an American National Standard on this subject. Suggestions for revision should be directed to: Standards & Technology Department, Telecommunications Industry Association, 2500 Wilson Boulevard, Arlington, VA 22201 U.S.A.

(From Project No. 3-0109, formulated under the cognizance of the TIA TR-34 Committee on Satellite Equipment & Systems.)

Published by

©TELECOMMUNICATIONS INDUSTRY ASSOCIATION 2003
Standards & Technology Department
2500 Wilson Boulevard
Arlington, VA 22201 U.S.A.

PRICE: Please refer to current Catalog of
TIA TELECOMMUNICATIONS INDUSTRY ASSOCIATION STANDARDS
AND ENGINEERING PUBLICATIONS
or call Global Engineering Documents, USA and Canada
(1-800-854-7179) International (303-397-7956)
or search online at http://www.tiaonline.org/standards/search_n_order.cfm

All rights reserved
Printed in U.S.A.

NOTICE OF DISCLAIMER AND LIMITATION OF LIABILITY

The document to which this Notice is affixed (the "Document") has been prepared by one or more Engineering Committees or Formulating Groups of the Telecommunications Industry Association ("TIA"). TIA is not the author of the Document contents, but publishes and claims copyright to the Document pursuant to licenses and permission granted by the authors of the contents.

TIA Engineering Committees and Formulating Groups are expected to conduct their affairs in accordance with the TIA Engineering Manual ("Manual"), the current and predecessor versions of which are available at http://www.tiaonline.org/standards/sfg/engineering_manual.cfm. TIA's function is to administer the process, but not the content, of document preparation in accordance with the Manual and, when appropriate, the policies and procedures of the American National Standards Institute ("ANSI"). TIA does not evaluate, test, verify or investigate the information, accuracy, soundness, or credibility of the contents of the Document. In publishing the Document, TIA disclaims any undertaking to perform any duty owed to or for anyone.

The use or practice of contents of this Document may involve the use of intellectual property rights ("IPR"), including pending or issued patents, or copyrights, owned by one or more parties. TIA makes no search or investigation for IPR. When IPR consisting of patents and published pending patent applications are claimed and called to TIA's attention, a statement from the holder thereof is requested, all in accordance with the Manual. TIA takes no position with reference to, and disclaims any obligation to investigate or inquire into, the scope or validity of any claims of IPR.

TIA does not enforce or monitor compliance with the contents of the Document. TIA does not certify, inspect, test or otherwise investigate products, designs or services or any claims of compliance with the contents of the Document.

ALL WARRANTIES, EXPRESS OR IMPLIED, ARE DISCLAIMED, INCLUDING WITHOUT LIMITATION, ANY AND ALL WARRANTIES CONCERNING THE ACCURACY OF THE CONTENTS, ITS FITNESS OR APPROPRIATENESS FOR A PARTICULAR PURPOSE OR USE, ITS MERCHANTABILITY AND ITS NON-INFRINGEMENT OF ANY THIRD PARTY'S INTELLECTUAL PROPERTY RIGHTS. TIA EXPRESSLY DISCLAIMS ANY AND ALL RESPONSIBILITIES FOR THE ACCURACY OF THE CONTENTS AND MAKES NO REPRESENTATIONS OR WARRANTIES REGARDING THE CONTENT'S COMPLIANCE WITH ANY APPLICABLE STATUTE, RULE OR REGULATION, OR THE SAFETY OR HEALTH EFFECTS OF THE CONTENTS OR ANY PRODUCT OR SERVICE REFERRED TO IN THE DOCUMENT OR PRODUCED OR RENDERED TO COMPLY WITH THE CONTENTS.

TIA SHALL NOT BE LIABLE FOR ANY AND ALL DAMAGES, DIRECT OR INDIRECT, ARISING FROM OR RELATING TO ANY USE OF THE CONTENTS CONTAINED HEREIN, INCLUDING WITHOUT LIMITATION ANY AND ALL INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, LITIGATION, OR THE LIKE), WHETHER BASED UPON BREACH OF CONTRACT, BREACH OF WARRANTY, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY OR OTHERWISE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE FOREGOING NEGATION OF DAMAGES IS A FUNDAMENTAL ELEMENT OF THE USE OF THE CONTENTS HEREOF, AND THESE CONTENTS WOULD NOT BE PUBLISHED BY TIA WITHOUT SUCH LIMITATIONS.

PLEASE!

DON'T VIOLATE
THE
LAW!

This document is copyrighted by the TIA and may not be reproduced without prior permission of the Telecommunications Industry Association. For information consult our website at http://www.tiaonline.org/about/faqDetail.cfm?id=18

Organizations may obtain permission to reproduce a limited number of copies through entering into a license agreement. For information, contact:

Global Engineering Documents
15 Inverness Way East
Englewood, CO 80112-5704 U.S.A. or call
U.S.A. and Canada 1-800-854-7179, International (303) 397-7956

TIA STATEMENT OF POLICY

The following statement of policy, reflecting the basic objectives of all standardization programs, shall be included in all TIA standards:

> "TIA standards are designed to serve the public interest by eliminating misunderstandings between manufacturers and purchasers, facilitating interoperability, interchangeability and improvement of products, and assisting the purchaser in selecting and obtaining the proper telecommunications product for his particular need. Existence of such standards shall not in any respect preclude any member or non-member of TIA from manufacturing or selling products not conforming to such standards."

> "Except as provided in the Engineering Manual, Standards are proposed or adopted by TIA without regard to whether their proposal or adoption may in any way involve patents on articles, materials, or processes. By such action, TIA does not assume any liability to any patent owner, nor does it assume any obligation whatever to parties adopting TIA standards, to parties manufacturing or selling products or services conforming to such standards or to users of such products or services. Other TIA rules respecting standards where patents are involved are contained in the Manual and should be read in conjunction with these Guides. Furthermore, in all cases specific requirements and restraints expressed elsewhere in these Guides must govern."

CONTENTS

Revision History ix

Foreword x

1 Overview 1
1.1 Scope 1
1.2 Objectives 1
1.3 Document Organization 1
1.4 References 2
1.5 Abbreviations, Definitions and Symbols 3
1.5.1 Abbreviations 3
1.5.2 Definitions 7
1.5.3 Symbols 10

2 System Architecture 13
2.1 Introduction 13
2.2 System Overview 13
2.2.1 Network Architecture 14
2.2.2 Network Interfaces 15
2.3 Remote Terminal Characteristics 16
2.3.1 PC-Hosted Remote Terminals 17
2.3.2 Self-Hosted Remote Terminals 19
2.3.3 Remote Terminal Operational States 20
2.4 IPoS Protocol Reference Model 20
2.4.1 Service Points and Primitives 22
2.5 Layer-wise Functional Partitioning 25
2.5.1 Network Adaptation Layer 25
2.5.2 Data Link Layer (DLL) 25
2.5.3 Physical Layer (PHY) 27
2.6 Layer Procedures 28
2.6.1 Commissioning Procedures 28
2.6.2 Procedures in Idle Mode 32
2.6.3 Transport Procedures 36

3 IPoS Physical Layer 43
3.1 Introduction 43
3.2 Physical Layer Overview 43
3.3 Radio Transmission 44
3.3.1 Operating Bands 45
3.3.2 Duplexing Methods 46
3.3.3 RF Channel Spacing 46
3.3.4 Inroute Nominal Bandwidth 47
3.3.5 Frequency Tuning 47
3.3.6 Frequency Stability 47
3.3.7 Output Power 47
3.3.8 Output Power Control 48
3.3.9 EIRP 48
3.3.10 Off-Axis EIRP Spectral Densities 48

3.3.11 Carrier on EIRP ... 49
3.3.12 Unwanted Emissions ... 49
3.3.13 In-Band Unwanted Emissions ... 49
3.3.14 Antenna ... 50
3.3.15 Copolar Antenna Sidelobes ... 51
3.3.16 Cross-Polar Antenna Sidelobes ... 52
3.3.17 Phase Noise Specifications ... 52
3.3.18 Illustrative Example Link Budgets ... 52
3.4 Outroute Physical Layer ... 55
3.4.1 Modulation QPSK ... 56
3.4.2 Frame Structure ... 57
3.4.3 Scrambling ... 58
3.4.4 Channel Coding ... 58
3.5 Inroute Physical Layer ... 61
3.5.1 Modulation ... 62
3.5.2 Unique Words ... 63
3.5.3 Coding ... 64
3.5.4 Inroute Framing Structure ... 72
3.5.5 Burst Formats ... 73
3.6 Physical Layer Measurements ... 78
3.6.1 Outroute Bit Error Rate ... 78
3.6.2 Signal Quality Factor ... 78
3.7 Interface to Higher Layers ... 79
3.7.1 User Plane Primitives ... 79
3.7.2 Control Plane Primitives ... 80
3.7.3 Management Plane Primitives ... 81
3.8 Physical Layer Procedures ... 82
3.8.1 Timing Synchronization ... 82

4 Data Link Layer ... 85
4.1 Scope ... 85
4.2 Data Link Control Overview ... 85
4.3 Satellite Link Control Sublayer ... 86
4.3.1 Overview ... 86
4.4 Modes of Operation ... 87
4.4.1 Registration and Commissioning ... 87
4.4.2 IPoS Terminal Startup ... 87
4.4.3 IP Packet Delivery ... 88
4.5 Compression ... 88
4.6 Interface with Higher Layers: SI-SAP ... 88
4.6.1 Overview ... 88
4.6.2 User Plane ... 89
4.6.3 Control Plane ... 89
4.7 Media Access Control Sublayer ... 91
4.7.1 Overview ... 91
4.8 Interfaces, SAPs, Service Definitions, and Service Primitives ... 92
4.8.1 MAC Interface with Physical Layer ... 92
4.8.2 Interfaces with Layer Management Entities ... 92
4.8.3 Logical Interfaces with Peer Layer ... 93

4.9 Outroute Multiplexing ... 93
4.9.1 Transport Packet Header ... 94
4.9.2 Program Identifiers ... 95
4.10 Outroute MAC Sublayer ... 96
4.10.1 Outroute MAC Formats ... 96
4.11 Inroute MAC Sublayer ... 115
4.11.1 Inroute Logical Channels ... 117
4.11.2 Inroute Segmentation ... 128
4.12 MAC Procedures ... 134
4.12.1 System Timing ... 134
4.12.2 Remote Terminal Ranging ... 141
4.12.3 Inroute Group Selection by IPoS Remotes ... 145
4.12.4 Inroute Data Transmission Sequence ... 146
4.12.5 Contention Channel Access Procedures ... 149
4.12.6 Packet Filtering Procedures ... 150
4.13 Message Functional Definition and Contents ... 151
4.13.1 General ... 151
4.13.2 Packet Order of Presentation ... 151
4.13.3 Order of Bits Within a Field ... 152
4.13.4 Superframe Numbering Packet ... 152
4.13.5 Inroute Group Definition Packet (IGDP) ... 154
4.13.6 Inroute Command and Acknowledgment Packet (ICAP) ... 157
4.13.7 Bandwidth Allocation Packet ... 162
4.13.8 Inroute Acknowledgment Packet ... 164
4.13.9 Periodic Adapter Conditional Access Update (PACAU) ... 165
4.13.10 Interactive Conditional Access Update (ICAU) and Response (ICAU-R) ... 166
4.13.11 Periodic Element Broadcast (PEB) ... 167
4.14 Configurable Parameters ... 168

ANNEX A - (Normative): State Machines ... 169

ANNEX B - IPoS Security ... 185

FIGURES

Figure 2.2.1-1. IPoS System Architecture 15
Figure 2.3.1-1. IPoS PC-Hosted Terminal 18
Figure 2.3.2-1. IPoS Self-Hosted Terminal 19
Figure 2.4-1. Protocol Reference Model 20
Figure 2.4-2. Protocol Stack for U-Plane and C-Plane 22
Figure 2.4.1-1. Service Access Points 23
Figure 2.4.1-2. Primitive Flow 24
Figure 2.6.1.5-1. IPoS User Registration 31
Figure 2.6.2.1-1. IPoS System Information Reception 33
Figure 2.6.2.4-1. Bandwidth Request Allocation 36
Figure 2.6.3.1-1. Peer Layer PDU Exchanges 37
Figure 2.6.3.2-1. IPoS Outroute Data Flows 38
Figure 2.6.3.2-2. IPoS Inroute Data Flows 39
Figure 2.6.3.3-1. Traffic Channel Types 40
Figure 2.6.3.3-2. Control Channel Types 41
Figure 3.2-1. The Physical Layer and Its Relationship to the MAC Layer 44
Figure 3.3.18-1. Illustrative Example IPoS Outroute Link Budget (Forward) 53
Figure 3.3.18-2. Illustrative Example IPoS Inroute Link Budget (Return) 54
Figure 3.4-1. IPoS Outroute High-Level Functional Structure 55
Figure 3.4.1-1. QPSK Constellation 56
Figure 3.4.2-1. MPEG-2 Transport Mux Packet 57
Figure 3.4.2-2. Outroute Frame: Sync Bytes and Randomization Sequence R 57
Figure 3.4.3-1. Descrambler Diagram 58
Figure 3.4.4.1-1. Reed-Solomon (204,188, T=8) Error Protected Packet 59
Figure 3.4.4.1-2. Interleaved Frames; Interleaving Depth I = 12 59
Figure 3.5-1. High-Level IPoS Inroute Diagram 61
Figure 3.5.1-1. Block Diagram of the Modulator 62
Figure 3.5.3.1-1. Convolutional Coder Block Diagram 64
Figure 3.5.3.1.1-1. Data Format Entering Scrambler 65
Figure 3.5.3.2-1. IPoS Turbo Coder Block Diagram 66
Figure 3.5.3.2.3-1. Encoder Block Diagram for Parsed Parallel Concatenated Convolutional Codes 67
Figure 3.5.3.2.3.1-1. Constituent Encoder (Dotted Lines Effective for Trellis Termination Only) 68
Figure 3.5.4-1. Turbo Code Inroute Framing Structure 73
Figure 3.5.5.2-1. 64 ksps Convolutionally Coded Burst Elements 74
Figure 3.5.5.2-2. 128 ksps and 256 ksps Convolutionally and Turbo-Coded Burst Elements 75
Figure 3.5.5.2.1-1. IPoS Slot Frame Boundaries 75
Figure 3.5.5.2.1-2. Multiple Bursts Received Time Misalignment at IPoS Hub, 128 ksps and 256 ksps 76
Figure 3.6.2-1. Required Relationship Between E_{bt}/N_o and SQF 79
Figure 4.2-1. DLC Model 86
Figure 4.10.1.1-1. MAC Encapsulation of PSI Tables 98
Figure 4.10.1.1.4-1. DVB/MPEG-2 Transport Packet CRC-32 Decoder 102
Figure 4.10.1.2-1. MAC Encapsulation of Datagrams 103
Figure 4.10.1.3-1. IPoS MAC Address to MAC Header Mapping 107
Figure 4.11-1. Inroute MAC Encapsulation of Datagrams 116

Figure 4.11.1.1.4-1. CRC-16 Calculation....123
Figure 4.12.1.1-1. IPoS System Timing Relationships 136
Figure 4.12.1.2-1. "Ideal" and Actual SFNP Transmission Time at the Hub....137
Figure 4.12.2.4-1 Message Sequence for Remote Terminal Ranging....145
Figure 4.13.2-1. Packet Byte and Bit Order of Presentation 151
Figure 4.13.3-1. Order of Bits Within a Field 152

TABLES

Table 2.3-1. IPoS Terminals Typical Characteristics 17
Table 2.3.1-1. Typical IPoS PC-Hosted Terminal Characteristics 18
Table 2.3.2-1. Typical Self-Hosted/Gateway Features 19
Table 3.3.3-1. Outroute Channel Spacing for Sample Symbol Rates 46
Table 3.3.4-1. Inroute Channel Spacing for Sample Symbol Rates 47
Table 3.3.7-1. Output Power Requirement 48
Table 3.3.8-1. Output Power Control Requirement 48
Table 3.3.9-1. Typical EIRPs 48
Table 3.3.13.3-1. Limits of Radiated Field Strength at a Test Distance of 10 Meters in a 100 kHz Bandwidth 49
Table 3.3.13.3-2. Limits of Spurious Field Strength Transmission Disabled State 50
Table 3.3.13.3-3. Limits of Spurious Transmissions 50
Table 3.3.17-1. Suggested IPoS Reference Source Phase Noise 52
Table 3.4.4.2-1. Punctured Code Definition 60
Table 3.4.4.4-1. Receiver Demodulator Performance Requirements (Including Implementation Losses) 61
Table 3.5.1-1. OQPSK Signal Mapping 63
Table 3.5.3.1.3-1. Convolutional Encoder G2 Matrix 66
Table 3.5.3.2.3.3-1. Parameters R and C for Various Interleaver Size 70
Table 3.5.3.2.3.3-2. Values for Various Interleaver Size 70
Table 3.5.3.2.4-1. Channel Interleaver Sizes (Example) 72
Table 3.5.4.1-1. IPoS Inroutes TDMA Characteristics 73
Table 3.5.5.2.2-1. Burst Structure for 64 ksps 76
Table 3.5.5.2.3-1. Burst Structure 128 ksps - Convolutional 76
Table 3.5.5.2.4-1. Burst Structure for 128 ksps - Turbo 77
Table 3.5.5.2.5-1. Burst Structure for 256 ksps Convolutional 77
Table 3.5.5.2.6-1 Burst Structure for 256 ksps Turbo 78
Table 3.6.2-1. Required Relationship Between E_{bt}/N_o (dB) and SQF 78
Table 4.9.1-1. DVB/MPEG Transport Packet Header 94
Table 4.9.2-1. PID Range 95
Table 4.9.2-2. IPoS Default PIDs 96
Table 4.10.1.1.1-1. SI Section Header 99
Table 4.10.1.1.3-1. Outroute IPoS Data Broadcast Descriptor 100
Table 4.10.1.2.1-1. Outroute MAC Header 104
Table 4.10.1.2.2-1. Outroute IPoS MAC PDU Format 105
Table 4.10.1.3.1-1. Unicast MAC Address 108
Table 4.10.1.3.1-2. IPoS Unicast MAC Address Examples 108
Table 4.10.1.3.2-1. Multicast MAC Address 109
Table 4.10.1.3.2-2. IPoS Multicast MAC Address Examples 109
Table 4.10.1.3.3-1. IPoS Superframe Numbering Address 110
Table 4.10.1.3.4-1. IPoS Return Broadcast MAC Address Examples 110
Table 4.10.1.3.5-1. IPoS Return Group MAC Address Examples 110
Table 4.10.1.3.6-1. IPoS Unicast Conditional Access MAC Address Examples 111
Table 4.10.1.3.7-1. IPoS Multicast Conditional Access Address Examples 111
Table 4.10.1.4-1. Classification of IPoS Logical Channels 112
Table 4.11-1. Burst Payloads 117
Table 4.11.1.1-1. Inroute MAC PDU Format 118
Table 4.11.1.1.1-1. MAC Header for Convolutional Coding (Unallocated) 118

Table 4.11.1.1.2-1. MAC Header for Turbo Coding (Unallocated) 120
Table 4.11.1.1.3.1-1. Reset Indication Format 122
Table 4.11.1.1.3.2-1 Ranging Request Format 122
Table 4.11.1.2-1. Inroute MAC PDU Format 124
Table 4.11.1.2.1-1. MAC Header for Allocated Channels with Convolutional Coding 125
Table 4.11.1.2.2-1. MAC Header for Allocated Channels with Turbo Coding 126
Table 4.11.2.1-1. Start Fragmentation Header – Beginning of MAC PDU 129
Table 4.11.2.2-1. Start Fragmentation Header Offset – in MAC PDU 130
Table 4.11.2.3-1. Continuation Fragmentation Header – Beginning of MAC PDU 132
Table 4.11.2.4-1. Continuation Fragmentation Header – Offset in MAC PDU 132
Table 4.13.4-1. SFNP Message Format 152
Table 4.13.5-1. IGDP Message Format 155
Table 4.13.6-1. ICAP Message Format 157
Table 4.13.6.1-1. Ranging Acknowledgment Command 158
Table 4.13.6.2-1. Aloha Acknowledgment Command 159
Table 4.13.6.3-1. Disable/Enable IPoS Terminal Command 160
Table 4.13.6.4-1. Start Ranging Command 160
Table 4.13.6.5-1. Go Active Command 161
Table 4.13.6.6-1. Change Inroute Group Command 161
Table 4.13.6.7-1. Reset Terminal Command 162
Table 4.13.7-1. BAP Message Format 163
Table 4.13.7-2. Format of the Burst_allocation_record 163
Table 4.13.8-1. IAP Message Format 164
Table 4.13.9-1. PACAU Header Format 165
Table 4.13.9-2. PACAU Group Key Entry Format 165
Table 4.13.9-3. PACAU Element Key Entry Format 165
Table 4.13.10-1. ICAU Request 166
Table 4.13.10-2. ICAU Response Header 166
Table 4.13.10-3. ICAU Group Key Entry Format 167
Table 4.13.10-4. ICAU Element Key Entry Format 167
Table 4.13.11-1. PEB Format 167

REVISION HISTORY

Date	Revision Number	Comments
May 8, 2003	Version 0.1	Previous contributions have been consolidated for this first draft of the IPoS standard.
June 19, 2003	Version 0.2	This is an updated draft incorporating additions, clarifications, and corrections received during the May ’03 and June ’03 meetings of the Working Group.
August 7, 2003	Version 0.3	Incorporates updates, corrections, and editorial improvements received during the June ’03 and August ’03 meetings.
August 26, 2003	Ballot Version 0.4	This version includes improvements received during the August ’03 meeting and the submission for ballot approval to TR34.1 on August 26, 2003.
September 8, 2003	Ballot Version 0.5	Includes updates received before the submission of the ballot version.
October 9, 2003	Publication Version 1.0	This version Includes Ballot comments received during the Ballot period from September 8, 2003 to October 8, 2003 and editorial corrections.

FOREWORD

(This foreword is not part of the standard)

This standard specifies the satellite air interface standard to be used to support the delivery of IP satellite services between remote terminals and the satellite access networks' hub of satellite access networks based on commercial Ku-band geosynchronous satellites. Throughout the remainder of this document, the term IPoS is used to refer to the satellite air interface and the satellite access networks compliant with this standard.

This specification is oriented primarily toward requirements necessary for the design of remote terminals. The hub is described only to the extent necessary to understand the remote terminal specifications. Additional requirements not covered in this document are needed for the hub design.

This document was prepared by the Satellite Communications Division, Working Group TR 34.1.7, of the Telecommunications Industry Association (TIA).

This page intentionally left blank.

1 OVERVIEW

1.1 Scope

This document contains the procedures used by remote terminals and the hub for delivery of traditional Internet Protocol (IP) services in a star satellite access network.

Remote terminals built to the parameters and procedures specified in this document can be used to create satellite access networks using commercial Ku-band geostationary, nonprocessing transponders with footprints within the United States of America or any other part of the world.

1.2 Objectives

The purpose of this document is to assemble the parameters and procedures permitting remote terminals from a variety of manufacturers to be compatible and to obtain services from satellite access networks conforming to this standard. To ensure this compatibility, this standard defines the essential parameters, formats, and procedures to a level that creates the same response from the remote terminals without constraining the particular implementation.

Enhanced capabilities such as performance enhancing proxies (PEPs) are not defined in this version of the standard.

1.3 Document Organization

This document is organized into four sections and two annexes:

Section 1, Overview: This is an introductory section that contains the document's organization, references, and definitions of terms.

Section 2, System Architecture: This section describes the major elements and interfaces in the IP over Satellite (IPoS) system and the organization of the satellite air interface between remote terminals and the hub.

Section 3, Physical Layer: This section describes the RF parameters, modulation, framing, and synchronization.

Section 4, MAC/SLC Layer: This section includes the procedures and formats used to encapsulate user and control information across the satellite air interface.

Annex A, State Machine: This annex shows the state machines for several of the processes executed by the remote terminals.

Annex B, IPoS Security: This annex describes the creation and distribution of various encryption keys used to provide the authentication of users and the

confidentiality of the information exchanged across the satellite interface in the IPoS system.

1.4 References

The following documents contain provisions that, through references in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or nonspecific.
- For a specific reference, subsequent revisions do not apply.
- For a nonspecific reference, the latest version applies.

References for sections 2, 3, 4, and Annex B are:

[1] ISO/IEC 13818-1, "Information Technology - Generic Coding of Moving Pictures and Associated Audio Information Systems: Part 1: Systems."

[2] ETSI TR 101 984 V1.1.1, "Satellite Earth Stations and Systems; Broadband Satellite Multimedia: Services and Architecture."

[3] IETF RFC 791, "Internet Protocol," Sept. 1981.

[4] IETF RFC 1883, "Internet Protocol, Version 6 (IPv6)," Dec. 1995.

[5] FCC Rule 25.209 on Antenna Performance Standards.

[6] ETSI EN 301 428 v1.2.1 (2000-12).

[7] ETSI EN 300 421 v1.1.2, "Digital Video Broadcasting (DVB); Framing Structure, Channel Coding and Modulation for 11/12 GHz Satellite Service."

[8] Forney, G.D. IEEE Trans. Comm. Tech., COM-19, pp. 772-781, (October 1971): "Burst-Correcting Codes for the Classic Bursty Channel."

[9] ITU-R P.618-6, "Propagation Data and Prediction Methods Required for the Design of Earth-Space Telecommunication Systems."

[10] "Electromagnetic Wave Propagation Through Rain, Robert Crane," John Wiley & Sons, February 1996, ISBN: 0-471-61376-2.

[11] ETSI EN 300 468, "DVB, Specification for System Information (SI) in DVB Systems."

[12] ETSI EN 301 192, v1.2.1 (1999-06), "DVB, DVB Specification for Data Broadcasting."

[13] ISO/IEC 13818-6, "Information Technology - Generic Coding of Moving Pictures and Associated Audio Information - Part 6: Extensions for DSM-CC."

[14] IEEE Standard 802.3, "Carrier Sense Multiple Access with Collision Detection and Supplement (CSMA/CD)."

[15] IETF RFC 1112, "Host Extensions for IP Multicast."

[16] ETSI TR 101 202, "DVB, Implementation Guidelines for Data Broadcasting."

[17] ETSI ETS 300 802, "DVB, Network Independent Protocols for DVB Interactive Services."

[18] IETF RFC 3135, "Performance Enhancing Proxies Intended to Mitigate Link-Related Degradations," June 2001.

1.5 Abbreviations, Definitions and Symbols

1.5.1 Abbreviations

For the purposes of the present document, the following abbreviations apply:

Adj	adjacent
Agg	aggregate
AIBO	aggregate input backoff
Ant	antenna
AOBO	aggregate output backoff
ARQ	Automatic Repeat Request
Atmos	atmospheric
Attn	attenuation
BAP	Bandwidth Allocation Packet
BAR	Bandwidth Allocation Request
BER	bit error rate
BO	backoff
bps	bits per second
BurstNr	burst number
BW	bandwidth
CBR	constant bit rate
CBC	cipher block chaining
CCITT	Consultative Committee for International Telegraphy and Telephony
CE	constant envelope
CE-OQPSK	constant envelope-offset quadrature phase-shift keying
C/N	carrier to noise
CON	confirm
CONUS	contiguous United States
CoS	Class of Service

C-Plane	control-plane
CRC	cyclic redundancy check
Crr	carrier
CSMA/CD	carrier sense multiple access with collision detection
CW	continuous wave
D/A	digital to analog
DES	Data Encryption Standard
DiffServ	differentiated services
DLC	data link control
DLL	data link layer
DNS	domain name server
DSM-CC	digital storage media command and control
DstIP	destination IP address
DVB	digital video broadcasting
DVB-S	digital video broadcasting via satellite
EBU	European Broadcasting Union
EEK	encrypted element key
EEMK	encrypted effective master key
EGK	encrypted group key
EIRP	effective isotropic radiated power
EK	element key
elv	elevation
EMK	effective master key
E/S	earth station
ETSI	European Telecommunication Standards Institute
ETSI DTS/SES	European Telecommunication Standards Institute Data Transport Service/Satellite Earth Stations
ETSI EN	European Telecommunication Standards Institute European Standard
ETSI ETS	European Telecommunication Standards Institute European Telecommunication Standard
ETSI TR	European Telecommunication Standards Institute Technical Report
FCC	Federal Communications Commission
FEC	forward error correction
FIFO	first in, first out
FIR	Finite Impulse Response
FLL	frequency lock loop
FSS	fixed satellite services
FTP	File Transport Protocol
GEO	Geostationary Earth Orbit
GK	group key
G/T	gain-to-noise temperature of the receiver
HPA	high power amplifier
HTTP	Hypertext Transport Protocol

I	interference
IAP	inroute allocation packet
IB	interleaver B
IC	interleaver C
ICAP	inroute command/acknowledgment packet
ICAU	interactive conditional access update
ICAU-R	interactive conditional access update response
ICMP	Internet Control Message Protocol
ID	identification, identities, or identifier
IDU	indoor unit
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IETF RFC	Internet Engineering Task Force Request for Comment
IF	intermediate frequency
IGDP	inroute group definition packet
IGMP	Internet Group Management Protocol
Im	Intermodulation
IND	indication
IntServ	integrated services
IP	Internet Protocol
IPoS	Internet Protocol over Satellite
IPsec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IR	Interleaver R
IRD	integrated receiver decoder
IRU	indoor receive unit
IS	Interleaver S
ISO	International Organization for Standardization
ITU	indoor transmit unit
LAN	local area network
LLC	logical link control
LNA	low noise amplifier
LSB	least significant bit
MAC	media access control
Max	maximum
MF-TDMA	multi-frequency time division multiple access
Min	minimum
Mis	miscellaneous
MK	master key
MPEG	Motion Pictures Expert Group
M-Plane	management plane
MSB	most significant bit
NACK	negative acknowledgment
NAT	Network Address Translation
NMC	Network Management Center
No.	Number

ODU	outdoor unit
OQPSK	offset quadrature phase-shift keying
OSI	open systems interface
PA	power amplifier
PACAU	periodic adapter conditional access update
PAT	Program Association Table
PC	personal computer
PDU	protocol data unit
PEB	periodic element broadcast
PEP	performance enhancing proxy
PHY	physical layer
PID	program identifier
PIM-SM	Protocol-Independent Multicast-Sparse Mode
PMP	point to multipoint
PMT	Program Map Table
PRBS	pseudorandom binary sequence
PSI	packet system information
PtP	point-to-point
PWM	pulse-width modulation
Pwr	power
QEF	quasi-error free
QoS	Quality of Service
QPSK	quadrature phase-shift keying
RAM	random access memory
REQ	request
RES	response
RF	radio frequency
RFC	Request for Comment
rms	root-mean-square
RS	Reed-Solomon code
RX	receive
SAP	service access point
SDNAL	satellite dependent network adaptation layer
SDU	service data unit
SeqNr	Sequence number
SerIP	Service Internet Protocol
SerNr	serial number
SF	superframe
SFD	satellite flux density
SFNP	superframe numbering packet
$SFNP_N$	superframe numbering packet that marks frame N (superframe number = N/8)
SI	service information
SI-SAP	satellite independent-service access point
SLC	satellite link control
SNAP	Subnet Access Protocol

SOHO	small office, home office
SQF	signal quality factor
SrcIP	source IP address
ST	satellite terminal
sync	synchronization
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TDM	time division multiplexing
TDMA	time division multiple access
Temp	temperature
TIA	Telecommunications Industry Association
TK	traffic key
TX	Transmit
UDP	User Datagram Protocol
U-Plane	user-plane
USB	universal serial bus
UW	unique word
VSWR	voltage standing wave ratio
Xmission	transmission
XOR	exclusive ORs
Xpol	cross-polarization
Xponder	transponder

1.5.2 Definitions

For the purposes of the present document, the following terms and definitions apply:

Access network: A satellite, cable, wireline, or wireless network that provides data transport facilities (satellite, cable, wireline, or wireless) and resources (IP addresses, DNS service) needed to provide IP-based services to remote users.

Aloha: An access method to inroute channels where remote terminals transmit with no bandwidth assignments from the hub. Conflicting transmissions are rescheduled by the remote terminals at a later time using a random backoff mechanism.

Always on: Type of service that maintains the subscriber session active over the IPoS satellite access network after the subscriber is registered in the satellite access network.

Automatic Repeat Request (ARQ): Error detection and correction mechanism that provides error correction by retransmission.

Best effort: Type of service that delivers packets from source to destination without QoS guarantees.

Cyclic Redundancy Check (CRC): A class of linear error detection codes that generate check bits by finding the remainder of a polynomial division.

Differentiated Services (DiffServ): An approach to provide QoS guarantees in the Internet where packets are classified into a small number of service classes by encoding the field in the IP header designated Differential Services Code Point.

Digital Video Broadcasting (DVB) ®[1]: DVB is an ITU-specified transmission scheme that supports the transfer of MPEG-2 compressed video, audio, program guides, and packet data that is adopted in the outroute direction of IPoS.

Domain Name Servers (DNS): DNS is a distributed database that maps Internet names to IP addresses.

Ethernet: Ethernet is a Local Area Network (LAN) technology that uses 48-bit addresses to identify the host computers connected to the LAN. Information over Ethernet is encapsulated into units called frames. The Ethernet frame has a 14-byte header that includes two 48-bit addresses (source and destination) and the length/type of the payload.

Forward Error Correction (FEC): Method to enhance the robustness of transmissions by using additional bits to protect the information units.

Inroute group: A set of inroute carriers that use the same physical layer (PHY) parameters, such as transmission rate and coding scheme, for the group of logical control and traffic channels supported by the inroute group.

Integrated Services (IntServ): An approach to provide sensitive applications with QoS guarantees based on reserving specific resources at every router traversed by the data flows of the application requesting preferential treatment.

Layering: A method of organizing the description of communication protocols into groups of decoupled processing entities or functions. There is no requirement to implement layering.

Logical channel: A communication path between the hub and the remote terminals described in terms of direction, connectivity, and the intended use of the information transferred.

Multicast: A service that delivers packets from a sender to a group of receivers. IPoS provides multicast by the hub transmitting only one copy of each packet for each multicast group over the outroute direction.

Multiprotocol Encapsulation: DVB-compliant specification that supports the transmission of IP datagrams over broadcast networks.

Network Address Translation (NAT): NAT is an Internet procedure that translates between two different sets of addresses, typically a set of globally registered IP addresses for external traffic and a second set of private addresses used for internal traffic in an access network or a LAN.

[1] DVB is a registered trademark of the DVB Project.

Performance Enhancing Proxy (PEP): An approach for improving the performance of TCP/IP over satellite links by inserting the PEP function at the hub and the desired remote terminals. PEPs operate above the DLC layer attempting to hide the losses and delays of the underlying satellite link from the end-to-end TCP/IP protocol.

Private IP network: A network that reuses the IP address space by being isolated from the global Internet. Private IP networks might be connected to the global Internet through a service gateway that provides the translation between private IP and global IP addresses.

Protocol stack: A conceptual model of a communication protocol using sequential layers that are represented in a vertical group or stack with the lower layer at the bottom of the stack.

Protocol Data Unit (PDU): Format used to encapsulate the data transferred between peer layers at the hub and remote terminals.

Punctured code: An error-correcting code derived from another error correcting code by deleting or puncturing coded bits from the output of the encoder.

Reserved: When used in connection with IPoS message fields, the term reserved means that the bits in these reserved fields might be used in future extensions. Unless otherwise specified, all reserved bits shall be set to binary value '0'.

Satellite link: A physical connection across satellite transponders that a transport protocol uses to communicate between remote users and the hub in a satellite access network.

Service Access Point (SAP): Conceptual point at the interface between adjacent protocol layers where data and protocol information are exchanged.

Sublayer: The result of decomposing a protocol layer into smaller function groupings.

Systematic encoder: An encoder, the output of which includes the input information bits followed by the parity bits created by the encoder to provide a more reliable information transfer.

Transmission Control Protocol/Internet Protocol (TCP/IP): TCP is the most common transport protocol, using the unreliable IP for moving packets and datagrams from a source to a destination in terrestrial IP networks. TCP is a window-based acknowledgment and flow control protocol that uses timeouts, sends and receives acknowledgments, and performs retransmissions to provide end-to-end reliable transmissions across multiple networks.

Turbo codes. Turbo encoders are structured with parallel concatenations of systematic convolutional encoders, the constituent encoders, with interleavers at the input of the constituent encoders. Turbo decoding uses an iterative decoding to achieve very good error-correction performance.

User Datagram Protocol (UDP): An unreliable protocol where one end sends datagrams without any preliminary connection establishment or subsequent acknowledgments.

Universal Serial Bus (USB): Standard computer interface used to interconnect PCs to peripheral devices. USB is a bit-serial bus with speeds from 12 Mbps in the older USB 1.0 and USB 1.1 versions and up to 480 Mbps in the latest USB 2.0. version.

Upper layers: General reference to protocol layers above the highest layer in the satellite network access stack. Examples are terrestrial transport layers such as TCP and UDP and application protocols such as HTTP, FTP, and e-mail.

1.5.3 Symbols

For the purposes of the present document, the following symbols apply:

/ or :	division
x or *	multiplication
| . |	indicates absolute value
'.'	single quotation mark used to represent binary fields
α	rolloff factor for a root raised cosine shaped filter
ΔT	change in time
π	angular 180 degrees
θ	angle in degrees from the axis of the mainlobe of the antenna
μs	microsecond
°	angular degrees
°C	temperature in degrees Centigrade
0x	prefix used to represent hexadecimal numbers
BT	bandwidth times symbol duration product
cm	centimeter
dB	decibel
dBμV/m	field strength measured as its ratio (in dB) to one microvolt/m
dBi	decibels over an isotropic radiator
dB/K	gain-to-noise temperature of receivers in dB

dBm	power expressed as its ratio (in dB) to 1 milliwatt
dBc/Hz	noise power spectral density where the noise power in one Hz is expressed in dB relative to the power of the unmodulated carrier
dBm/Hz	power spectral density indicating the power expressed in dBm over one Hertz of bandwidth
dBW/kHz	power spectral density indicating the power expressed in dBW over one kilohertz of bandwidth
dBpW	power expressed as its ratio (in dB) to one picowatt (10^{-9} watts)
dBW	power expressed as its ratio (in dB) to one watt
dBW/m^2	power density indicating the power in dBW in 1 square meter
E(.)	exponential
E_{bi}	energy per information bit of the received signal at the output of the decoder
E_{bi}/N_o	ratio of the energy per information bit and the noise density at the output of the decoder expressed in dB
E_{bt}/N_o	ratio of energy per received bit and the noise density at the output of the demodulator (input to the decoder) expressed in dB
$EIRP_{max}$	maximum EIRP
f_N	Nyquist frequency
GHz	Gigahertz (10^9 Hertz)
hex	hexadecimal notation
H(f)	filter frequency response
h(t)	filter impulse response or shaping pulse waveform
Hz	Hertz
I	in-phase component of the modulated signal
j	imaginary unit
k	time index
K	Temperature in degrees Kelvin and convolutional code constraint length
kHz	kilohertz (10^3 Hertz)
ksps	kilosymbols per second

1	$\log_{10}$	decimal logarithm
2	m	meter
3	MHz	Megahertz (10^6 Hertz)
4	msec	millisecond
5	Msps	Megasymbols per second
6	N_o	Noise density (unit of bandwidth)
7	Q	quadrature component of the modulated signal
8	R_s	symbol rate
9	s	second
10	sps	symbols per second
11	Theta	angle designation; symbol is θ
12	T_{HO}	hub offset time
13	$T_{H\text{-}S}$	propagation time from hub to satellite
14	$T_{H\text{-}S\text{-}H}$	$T_{H\text{-}S\text{-}H} = T_{H\text{-}S} + T_{S\text{-}H}$
15	T_{RO}	remote terminal offset time
16	$T_{R\text{-}S}$	propagation time from remote terminal to satellite
17	$T_{S\text{-}H}$	propagation time from satellite to hub
18	Ts	symbol duration
19	W	watts

2 SYSTEM ARCHITECTURE

2.1 Introduction

This section is an introduction to the Internet Protocol over Satellite (IPoS) system. In particular it contains a high-level description of the different functional capabilities and services of the system and the remote terminals that give access to users of these services and capabilities in the IPoS system. This section also describes the protocol architecture adopted for the satellite interface between remote terminals and the hub through which user data and signaling information are transferred among the different functional layers of the remote terminal and the hub.

2.2 System Overview

The IPoS system delivers "always on" IP services via geosynchronous satellites primarily targeted to the following markets:

- Residential/Consumer: The primary service offered to consumers by IPoS is broadband Internet access, including traditional IP services such as e-mail, file transfer, and Web browsing based on Transmission Control Protocol/Internet Protocol (TCP/IP) with additional value-added IP multicast services such as video/audio streaming, distance learning, etc.

- Small office/home-office (SOHO): The primary IPoS service offered to the SOHO market is premium-level broadband Internet access, including the aforementioned value-added services.

This IPoS standard has been developed to create a multivendor procurement environment of remote terminals that results in efficient solutions for providing the two-way satellite Internet access transport capability required by these residential and SOHO markets. Key characteristics of this standard include:

- Terrestrial IP networks interoperability
- Easy scalability
- Universal applicability
- Easily deployable
- Comprehensive management capability

2.2.1 Network Architecture

IPoS is a star satellite network that encompasses three major segments:

1. Hub segment: The hub segment supports Internet access of a large number of remote terminals via satellite. It is composed of large hub earth stations and related equipment through which all traffic flows. The hub segment can be further broken down as follows:

    - An IPoS hub earth station is the large earth station through which many thousands of terminals communicate. A hub earth station exists at a single location, may access space segment resources from multiple satellites, and configures and manages from a single, centralized database.

    - An IPoS Network Management Center (NMC) is a single management center, collocated with the IPoS hub earth station that manages the entire IPoS system. The parts of the NMC that directly manage hub earth stations and terminals are considered to be components that are internal to the IPoS system.

    - The IPoS backend systems include, but are not limited to, routers, firewalls, Domain Name Servers (DNSs), etc. They provide the interface between the IPoS and the external public network, e.g., Internet.

2. Space segment: The space segment consists of bent-pipe transponders on geosynchronous satellites that allow transmission in both directions between the hub and remote terminals. IPoS parameters and procedures are somewhat independent of the underlying spectrum (whether C-band, Ku-band, Ka-band, or even X-band) used by the satellite transponders; however, there are physical requirements involving radio frequency parameters that are specific for each particular frequency band. The IPoS Physical Layer (PHY) interface in section 3 of this standard assumes IPoS services using Ku-band commercial satellites with spectrum that is designated for fixed satellite services (FSSs).

3. User segment: In general, the IPoS user segment consists of thousands of user terminals, each of them capable of providing broadband IP communications to a remote site. User terminals are also referred to in this standard as remote terminals. The remote terminals support the user hosts, or personal computers (PCs), running the applications. This support of user PCs could be broadly categorized:

    - Single access point: where the host and the remote terminal are connected, e.g., through a universal serial bus (USB) interface.

    - Customer premises LAN: where the remote terminals provide access to a multiplicity of PCs. Customer LANs are considered external to the IPoS system.

Figure 2.2.1-1 illustrates the highest-level components in the IPoS architecture and identifies the major internal and external interfaces in the IPoS system.

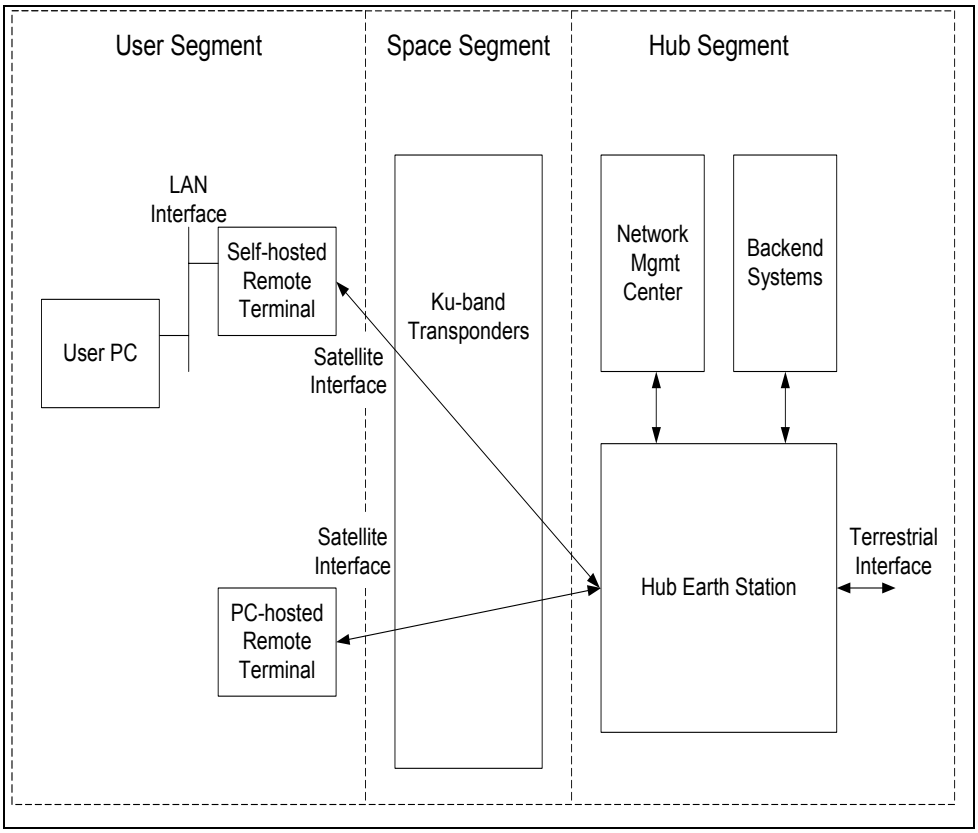


Figure 2.2.1-1. IPoS System Architecture

2.2.2 Network Interfaces

The main interfaces in the IPoS system are:

- Terminal LAN interface: This is the interface between the user hosts' computers, or PCs, and the remote terminals. The terminal LAN interface uses an Ethernet protocol that is not part of this standard.

- IPoS satellite interface: This is the interface where remote terminals and the hub exchange user, control, and management information. The IPoS satellite interface, or air interface, is the main focus of this standard.

- Hub terrestrial interface: This is the interface between the hub and the backbone connecting the hub to the external packet data networks, public Internet, or private data networks. The hub terrestrial interface uses IP protocols that are not part of this standard.

The IPoS satellite interface distinguishes between the two transmissions' directions:

- The outroute direction from the IPoS hub to the user terminals is broadcast over the entire bandwidth allocated to the outroute carrier. Because the IPoS outroute can multiplex a multiplicity of transmissions, it streams to many remote terminals.

- The inroute direction from the remote terminals to the IPoS hub is point-to-point (PtP), either using bandwidth assigned by the hub for individual remote terminals or using bandwidth shared by all terminals on a contention basis.

2.2.2.1 Outroute Satellite Transmission

IPoS outroute carriers use a statistical multiplexing scheme compliant with the DVB data format in reference [1] (found in subsection 1.4 of this document) for sharing the outroute among the remote terminals. The distribution of IP traffic to the remote terminals is based on the DVB multiprotocol encapsulation in reference [12]. Symbol rates from 1 Msps to 45 Msps are supported at forward error correction (FEC) Rates ½, 2/3, ¾, 5/6, and 7/8.

2.2.2.2 Inroute Satellite Transmission

An IPoS inroute uses offset quadrature phase-shift keying (OQPSK) modulation at transmission rates of 64, 128, or 256 ksps when using Rate ½ convolutional encoding or at transmission rates of 128 or 256 ksps when using Turbo FEC encoding.

IPoS uses demand-assigned MF-TDMA (multifrequency time division multiple access) on its inroutes to allow terminals to transmit to the hub. The IPoS inroute has a 45-millisecond TDMA frame length divided into a variable number of slots. Transmissions from a terminal to the hub are referred to as a “burst.” A burst requires an integral number of slots for overhead and then carries an integral number of slots of data. These overhead slots are used to provide the burst preamble and to allow adequate time between bursts to ensure that consecutive bursts do not overlap in time.

2.3 Remote Terminal Characteristics

The remote terminal is the access platform from which the user hosts access the services of the IPoS system. Whether or not a terminal requires the support of a PC is one of the critical methods used to categorize IPoS terminals. According to these criteria, there are two remote terminal categories:

1. PC-hosted: This type of terminal is primarily oriented toward consumer applications. PC-hosted remote terminals operate as a PC peripheral, typically a USB peripheral, and significant support from the PC is required for operation. This support includes:

- Downloading the peripheral's software
- Enabling performance enhancement function
- Commissioning and management functions

2. Self-hosted: Self-hosted terminals are aimed at consumer and SOHO market segments. The self-hosted remote terminals do not require an external PC to support their operation in the IPoS system. Self-hosted terminals could be fully managed by the hub, e.g., self-hosted remote terminals can have their software downloaded, and their configuration parameters set by the hub.

Another criterion for categorizing remote terminals is the type of return channel that a terminal uses to send data to the hub. Accordingly, remote terminals can be classified into:

- Satellite Return Channel: transmits back to the hub directly via the inroute satellite channels part of the IPoS system.
- Receive-Only with Terrestrial Return: operates receive-only with respect to the satellite, using some form of terrestrial return capability (e.g., a dial-up connection).

Table 2.3-1 summarizes typical characteristics of the various types of remote terminals currently defined in the IPoS system.

Table 2.3-1. IPoS Terminals Typical Characteristics

Terminal Name/Features	Hosting	Return Channel
Low-Cost, Two-Way, Broadband Satellite PC Peripheral	PC	Sat
Low-Cost, Two-Way, Broadband Self-Hosted Terminal	Self	Sat
Receive-Only, Lowest-Cost Satellite Broadband, PC Peripheral	PC	Dial-up

2.3.1 PC-Hosted Remote Terminals

The IPoS PC-hosted terminal typically consists of an outdoor unit (ODU) and an indoor unit (IDU) connected by two coaxial cables. See figure 2.3.1-1.

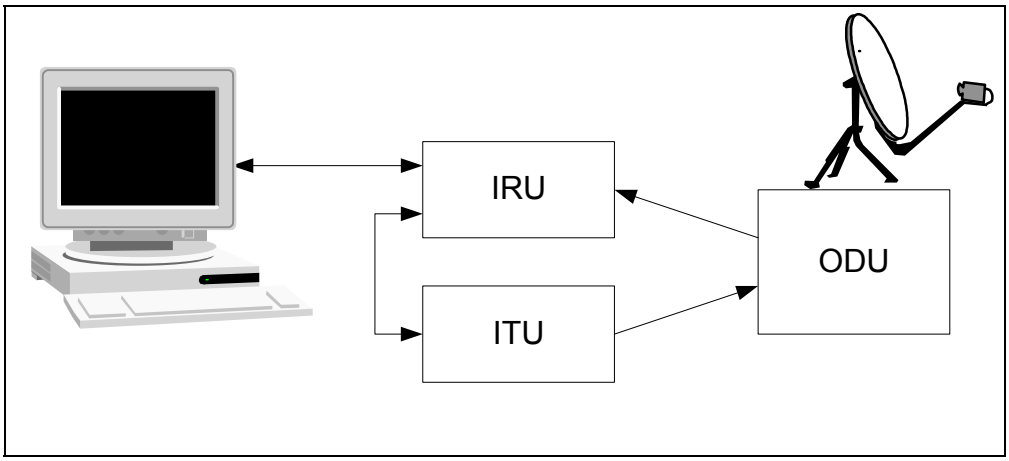


Figure 2.3.1-1. IPoS PC-Hosted Terminal

In a typical configuration, the indoor receive unit (IRU) and indoor transmit unit (ITU) may be integrated into a single box.

The ODU consists of an antenna with transmit and receive electronics. Depending on the size of the antenna, the satellite, and the specific propagation characteristics of the remote terminals location, the ODU might support up to 256 ksps inroute and multimegabits outroute transmission rates.

The PC-hosted terminal interfaces to the end-user PC, with the IRU acting as a USB 1.1 peripheral to the PC.

A satellite-based commissioning process, along with an auto-setup program, automatically installs and configures the TCP/IP stack and browser with the appropriate configuration parameters, including an IP address.

The IPoS PC-hosted terminal might use a combination of TCP PEP and Hypertext Transfer Protocol (HTTP) PEP to increase Internet access performance while reducing satellite capacity utilization. PEP is a suite of features that provides Web acceleration and other capabilities. See table 2.3.1-1 for typical characteristics of the PC-hosted remote terminals.

Table 2.3.1-1. Typical IPoS PC-Hosted Terminal Characteristics

PC Interface	USB 1.1, Throughput Exceeding 4.5 Mbps
Satellite receiver modulation specs	DVB-S to 45 Msps, R1/2-7/8 FEC
Antenna-to-indoor equipment interface	Dual RG-6 coax, one for RX, one for TX

2.3.2 Self-Hosted Remote Terminals

A self-hosted terminal also consists of an ODU and an IDU connected by two coaxial cables. The IDU contains a module that provides the user gateway functionality. See figure 2.3.2-1.

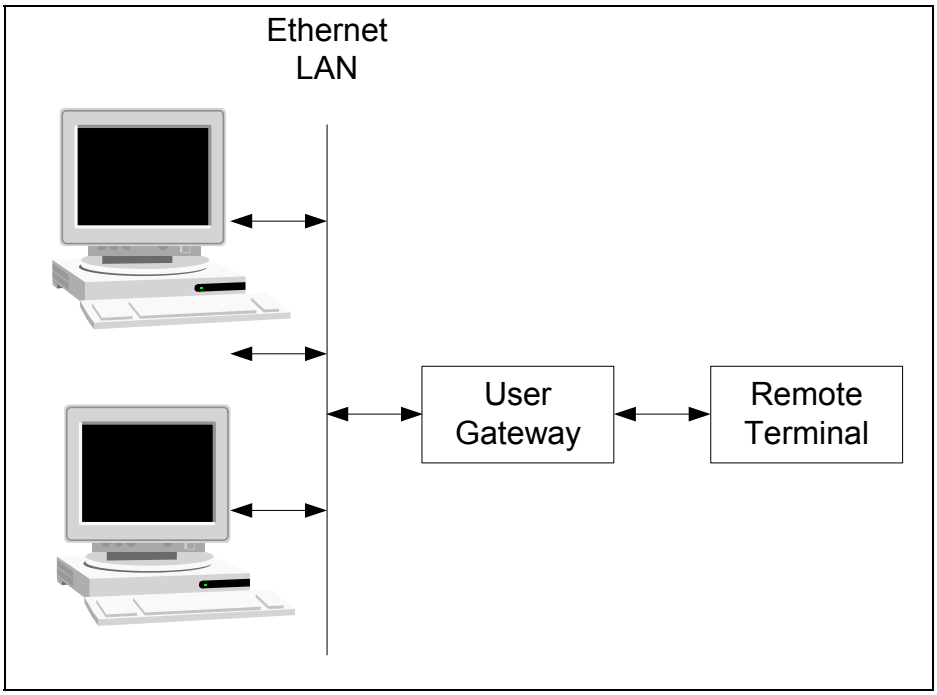


Figure 2.3.2-1. IPoS Self-Hosted Terminal

The user gateway replaces the PC in the PC-hosted remote terminal, to allow operation in a multi-PC environment found in both consumer and SOHO markets. The user gateway provides an Ethernet interface to LAN-based IP devices. The user gateway stores both the IRU's software and its own software in nonvolatile memory and is configured and managed by a network/element management system.

Typical features of self-hosted remote terminals are shown in table 2.3.2-1.

Table 2.3.2-1. Typical Self-Hosted/Gateway Features

Router/Gateway Features	Static routes to support other routers on the remote LAN ICMP (Internet Control Message Protocol) IGMP (Internet Group Management Protocol) – for the satellite IP multicast packets onto the LAN.
Interfaces	Ethernet (10/100BaseT) USB 1.1 (Type A)

2.3.3 Remote Terminal Operational States

The operational states determine the type functions performed by the remote terminals. Three main operational states are used in the operation of the remote terminals:

1. **Commissioning state**: In this state the remote terminal gets the configuration parameters, addresses, and encryption keys needed to contact the hub. At the end of the commissioning state, the remote terminal is registered, authenticated, and ready to receive information from the hub.

2. **Idle state**: In this state the remote terminals are an addressable entity that can receive system information and specific configuration parameters about the inroute direction. At the end of the Idle state, the remote terminals are ready for reaching the Active state.

3. **Active state**: In this state the remote terminal can execute secure and reliable transfer of user, control, and management information with the hub.

2.4 IPoS Protocol Reference Model

The IPoS protocol is a multilayered peer-to-peer protocol providing the mechanisms to exchange IP traffic and signaling information between the entities in the hub and remote terminals.

The IPoS protocol is structured according to the architecture in Reference [2] (found in subsection 1.4 of this document), which provides a split between satellite-dependent functions and satellite-independent functions, as illustrated in figure 2.4-1.

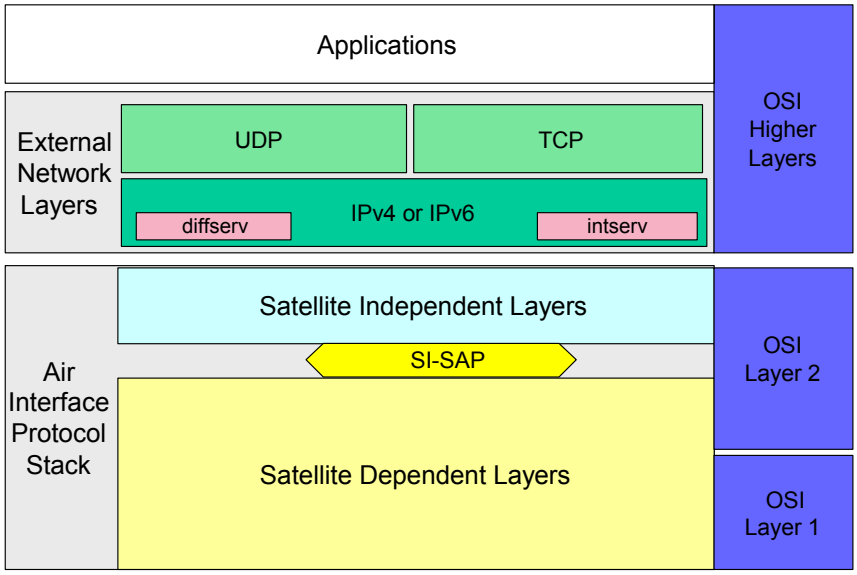


Figure 2.4-1. Protocol Reference Model

The protocol architecture separates satellite-dependent functions and satellite-independent functions via an interface designated the SI-SAP. The purpose of this split is as follows:

- Separate the satellite-specific aspects from the satellite-independent higher layer. This separation is designed to permit future market developments, in particular IP enhancements.

- Provide flexibility for the addition of more complex market segment-based solutions (e.g., PEPs).

- Elements above the SI-SAP can be ported with greater ease to new satellite systems.

- Extensibility to support new higher-layer functionalities without major reengineering of existing designs.

As shown in figure 2.4-1, the SI-SAP is positioned between the data link (layer 2) and network layers in the International Organization for Standardization (ISO) layering model. Elements above the SI-SAP can be, and indeed should be, designed without specific knowledge of the supporting satellite link layer. The satellite-independent layers in figure 2.4-1 are generic, including services not currently specified by IPoS such as IntServ, DiffServ, and IPv6.

The IPoS interface is organized into planes, layers, and directions of transmission over the satellite. There are three protocol planes:

1. User plane (U-Plane): provides the protocols needed for reliable transport of IP traffic containing user information across the satellite interface.

2. Control plane (C-Plane): contains the signaling protocols needed to support and control the satellite access connections and resources needed in the transport of user traffic.

3. Management plane (M-Plane): concerned with the administration and messaging related to the commissioning of remote terminals, the billing of the users, performance, and alarm reporting. The management plane is outside the scope of this standard.

Each of the IPoS planes is logically divided into three protocol sublayers. The protocol sublayers are used to decompose the overall system functionality into groupings of functions at the same abstraction level.

- Physical Layer (PHY): provides the lower-level functionality related to modulation, error control of the information, and signaling streams transported across the interface

- Data Link Control (DLC) layer: provides the multiplexing of the various streams as well as reliable and efficient transport services

- Network Adaptation Layer: controls user access to the satellite and controls radio resources needed for this access

In general, figure 2.4-2 shows the protocol organization of the IPoS interface in the U-Plane and C-Plane. The protocol stack separates the IPoS-specific protocol layer between the IPoS hub and the remote terminal from the IP and above end-to-end higher layers between host computers.

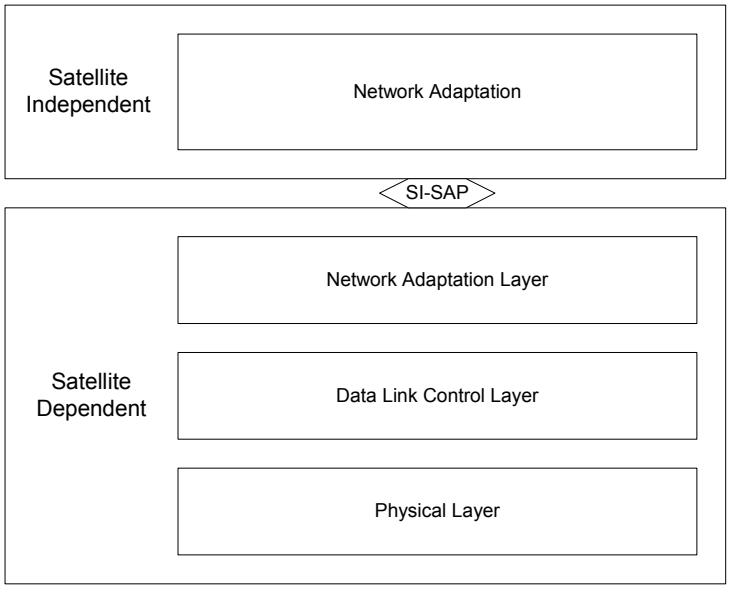


Figure 2.4-2. Protocol Stack for U-Plane and C-Plane

The layers in the IPoS system are divided into two directions of transmission, each of them associated to the highly asymmetric capabilities over the satellite bearer channels. The two directions are designated:

1. The outroute direction from the IPoS hub to user terminals is broadcast over the entire bandwidth allocated to the outroute carrier. Because The IPoS outroute can multiplex transmissions, it streams to many remote terminals.

2. The inroute direction from the remote terminals to the IPoS hub is PtP, either using bandwidth assigned by the hub to individual remote terminals or using bandwidth shared by all terminals on a contention basis.

2.4.1 Service Points and Primitives

Adjacent sublayers in the IPoS protocol architecture connect to each other through interface points, designated Service Access Points (SAPs). Through the SAPs the sublayers access the services and capabilities provided by the adjacent sublayer. In general, there are three SAPs at each layer; the SAPs are associated with the U-Plane, C-Plane, and M-Plane, as illustrated in figure 2.4.1-1.

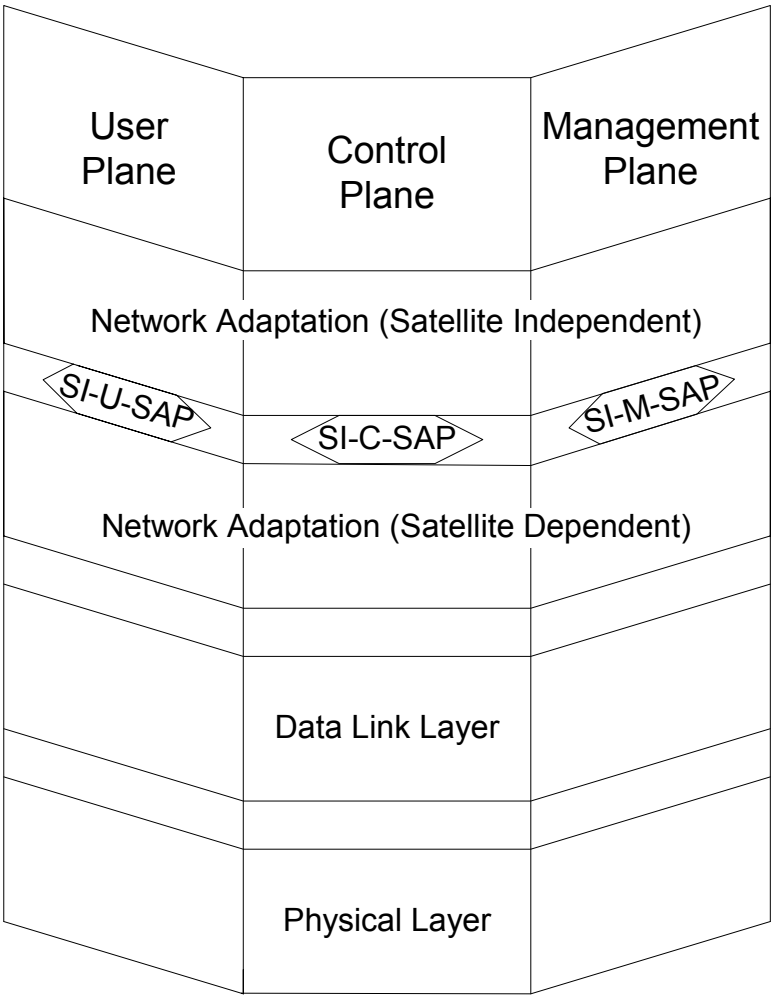


Figure 2.4.1-1. Service Access Points

Interactions between adjacent layers across SAPs are in terms of primitives. A primitive is an abstract representation of the information and control exchanges through the SAP. Four types of primitives are used in the IPoS interface to represent the passing information across the layers of the U-Plane and C-Plane. The actions implied by these primitives are:

1. Request (REQ): occurs when a higher layer invokes services or functions from the adjacent lower layer

2. Indication (IND): used by the lower layer to notify the higher layer of a REQ at the peer layer

3. Response (RES): carries the acknowledgment from the higher layer to the lower layer for an indication primitive

4. Confirm (CON): used by the lower layer to notify the higher layer that the requested service has been completed

The primitive type also indicates the direction of the flow of information. These flows are indicated in figure 2.4.1-2.

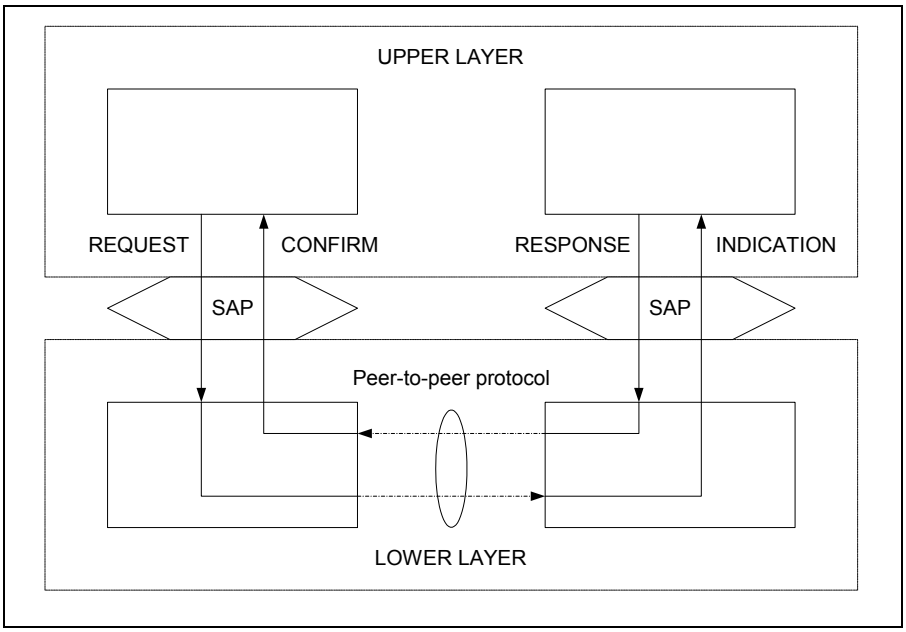


Figure 2.4.1-2. Primitive Flow

The general syntax of primitives in the IPoS contains the following four elements:

1. Sublayer
2. Plane
3. Generic Name
4. Type

where:

- Sublayer designates the initials of the sublayer or SAP, providing the services (PHY for physical, media access control (MAC) for the medium access layer, DLC for data link control, or SI for primitives across the SI-SAP interface).
- Plane designates the initial of the plane where the interaction occurs (U for U-Plane, C for C-Plane, or M for M-Plane).
- The Generic Name designates the type of service or function invoked, e.g., data for data transfer.
- Type designates the initials of the type of primitive, e.g., REQ, IND, RES, or CON.

For example, the primitive used by the satellite-independent layers to request the transfer of IP data by the IPoS DLC over the IPoS air interface is SI-U-DATA-REQ, and the primitive that the DLC uses to deliver an IP packet received over the IPoS air interface to the satellite-independent layers is SI-U-DATA-IND.

2.5 Layer-wise Functional Partitioning

This subsection gives the functional responsibilities for the layers in the satellite-dependent part of the IPoS interface.

2.5.1 Network Adaptation Layer

The Network Adaptation Layer function provides the following major subfunctions:

- IP Packet Transport: This function performs the functions necessary to determine the Class of Service of the IP packet based on packet type, application type, destination, and internal configuration.

- Traffic Management: This function performs the traffic shedding and policing functions on IP packets before they are offered to the IPoS transport services.

- PEPs: This function improves the performance of certain applications for improving service over a satellite link. PEPs are often used to reduce the degradations in throughput experienced by TCP applications because of the delays and losses in satellite links. Reference [18] (found in subsection 1.4 of this document) discusses various types of PEPs and the mechanisms they use to improve performance. Use of PEPs is optional in IPoS. Typically the PEP sits at the hub, splitting the end-to-end TCP transport link, acting as virtual TCP senders/receivers connecting the satellite access system from the terrestrial Internet to the satellite system. PEP is customized to match the characteristics of the IPoS satellite links.

- Multicast Proxy: This proxy adapts IP multicast protocols (e.g., PIM-SM) to the appropriate IPoS transport services to provide the multicast.

The Network Adaptation Layer is not part of the IPoS air interface specification.

2.5.2 Data Link Layer (DLL)

The DLL provides the actual transport service over the IPoS network. It is divided into the following sublayers:

- Satellite Link Control (SLC)
- Media Access Control (MAC)
- Outroute multiplexing sublayer

2.5.2.1 Satellite Link Control Sublayer

The SLC layer is the sublayer of the DLC that is responsible for transmission of packets between remote terminals and the hub.

IPoS supports different delivery methods over the outroute and inroute directions.

A reliable error-free delivery method is used in the inroute direction using selective retransmissions. In this reliable delivery method, the receiving SLC entities deliver only error-free data packets to the higher layers.

Over the outroute where the transmission errors are very low (typical BER = 1*E(-10), the transmit SLC delivers each data packet only once without retransmission of errored or missing packets.

The functional responsibilities of the SLC are:

- Generation of session IDs and mapping incoming packets into the corresponding session
- Encryption of specific IP PDUs (protocol data units) for user-to-user data privacy
- Segmentation and reassembly, which performs segmentation/reassembly of variable-length higher layer data packets into smaller PDUs
- Delivery of data in sequence to the peer using the reliable/unreliable mode of delivery

2.5.2.2 Medium Access Control Sublayer

The services or functions provided by the MAC layer can be grouped into the following categories:

- Data transfer: This service provides unacknowledged transfer of MAC interactions between peer MAC entities. This service does not provide any data segmentation; therefore, the upper layers provide the segmentation/reassembly function.
- Reallocation of radio resources and MAC parameters: This service performs control procedures for identifiers that are allocated to a particular DLC layer by the network layer for an interval of time or on a

permanent basis. It also performs procedures for the establishment and termination of transfer modes over the DLC layer.

- Error detection: Procedures for the detection of procedural errors or errors occurring during the transmission of frames.

2.5.2.3 Outroute Multiplexing Sublayer

In the outroute direction, the multiplexing sublayer permits the hub to transmit several traffic types, programs, or services within the same outroute carrier and controls the transmission of each individual program. The IPoS multiplexing sublayer is based on the Digital Video Broadcast /Motion Pictures Expert Group (DVB/MPEG) statistical multiplexing format in reference [1] (found in subsection 1.4 of this document). In this DVB/MPEG format, all the frames or packets associated with one of the traffic types have the same Program Identifier (PID). At the remote terminals, a demultiplexer breaks the outroute multiplex into specific transport streams with the remote terminal filtering only those that match the PID addresses configured in the terminal.

IPoS remote terminals are configured to filter two types of PIDs associated with the following types of transport streams, which are relevant to the IPoS system:

1. PSI tables, which provide both IPoS and non-IPoS terminals with configuration of services. The IPoS terminals receive the PSI tables to determine the specific configuration of the IPoS system.

2. IPoS user and control information, which is transported in the IPoS logical channels. The information contained in the IPoS logical channels can be targeted to all, a group, or individual IPoS terminals.

Outroute DVB/MPEG packets are broadcast over the entire outroute carrier bandwidth with IPoS terminals filtering those packets that do not match their own addresses. The addressing scheme is included as part of the transport packet header and MAC header.

2.5.3 Physical Layer (PHY)

The Physical Layer function provides the transmission and reception of the modulated waveforms used to transport the data provided by the data link and higher layers over the satellite. At the PHY, there is no distinction among the transport methods provided for U-Plane, C-Plane, or M-plane information. This distinction is made at higher layers.

The services provided by the PHY layer are grouped into the following categories:

- The initial acquisition, synchronization, and ranging procedures with the hub, including the timing alignment of the transmissions with the frame structure of the inroute carriers and the adjustment of the power transmitted by the remote terminals

- The modulation, coding, error correction, scrambling, timing, and frequency synchronization of information flows, provided by the DLC's U-Plane and C-Plane to the outroute and inroute carriers

- The performance of local measurements such as received E_{bt}/N_o, recovered clock, and status and supervision of the physical parameters (such as timing) and their reporting to higher layers

2.6 Layer Procedures

The IPoS system relies on a multiplicity of procedures and algorithms to perform its functionality. The subsections below identify the procedures used over the IPoS air interface. The procedures are divided into:

- Commissioning procedures: These are mainly M-Plane procedures concerned with the initial configuration of the remote terminals and database at the hub and the binding of addresses and encryption keys used to transfer data over the IPoS system to the individual remote terminals.

- Idle state procedures: These are mainly C-Plane procedures a terminal needs to perform before becoming active and in returning to the Idle state after exchanging traffic.

- Transport procedures: These are mainly U-Planes providing the reliable exchange of user, control, and management information in the Active state.

- Security procedures: These are procedures executed to protect the unauthorized use of services in the IPoS system and to provide encryption of the information transferred across the satellite.

In general, procedures involve one or more of the sublayers in the IPoS protocol architecture. The particular partitioning of procedures between sublayers is to a large extent an implementation issue.

2.6.1 Commissioning Procedures

The following describes the commissioning procedures needed to be performed before the terminal is ready to exchange traffic over the IPoS system. The parameters needed during the commissioning procedures (such as satellite location, transponder frequencies, addresses, and encryption keys) are determined by the IPoS network managers or at the factory.

2.6.1.1 Installation

The installation of the remote terminal is performed by a trained installer. The following parameters are configured during the installation:

- Satellite orbital location in degrees
- Characteristics of the outroute carrier to be used, i.e., such as frequency, symbol rate, modulation, and coding
- Transponder polarization
- The latitude and longitude of the IPoS remote being configured (alternatively a Post Code or ZIP code lookup table could be used)
- IP address of IP packet processor at the hub
- The remote terminal's own internal address within the system

The installer points the antenna and adjusts the antenna polarization plane to minimize cross-polarization interference.

2.6.1.2 System Timing

During the system timing procedure, the remote terminal uses parameters configured during installation to acquire and demodulate the outroute carrier and extract system timing and other relevant information conveyed by the outroute carrier.

The acquisition of the outroute carrier provides the remote terminal with:

- The symbol clock of the demodulated carrier to be used for the frequency stability of the local frequency reference used to derive the frequency of the inroute carriers
- Reception of the superframe numbering packets transmitted by the hub every 360 msec at the beginning of every superframe
- The PIDs used by the remote to prefilter the control and traffic information contained in the outroute
- The information in the channels with the PID addresses monitored for the terminal

2.6.1.3 Synchronization

Synchronization refers to the process of aligning the remote terminals' transmissions over the inroute direction with the reference timing of the inroute frames at the hub. During synchronization, the remote terminals calculate the initial timing offset needed to introduce the marker received from the superframe over the outroute carrier for the IPoS hub. This marker is needed so that the hub can receive the remote transmission assigned from the frame structure of the inroute carriers at the hub.

The IPoS remote uses rough location information (such as ZIP code or lat/long) from the remote site and the satellite ephemeris for an initial course estimation of the timing offset needed for inroute transmissions.

2.6.1.4 Ranging

Ranging is the process for obtaining a fine timing offset estimate for inroute transmissions. During the ranging procedure, the remote terminals transmit over specific inroute channels designated for this purpose. The hub receives the ranging bursts. The hub then estimates the timing adjustment needed to align the remote terminal's inroute transmissions and sends the adjustment to the remote.

Also, during ranging the hub estimates the power level of the remote and sets the inroute power of the remote terminal. The remote terminal supplies the hub within the Ranging Request with a measurement of the receive signal strength of the outroute carrier. The hub records this information along with other information about the remote terminal.

2.6.1.5 Registration

Registration is the process whereby authorized remote terminals are given the internal addresses. In addition, the terminals are also given the encryption keys needed at the hub to forward traffic to these terminals and for the remote terminals to decrypt the information and exchange traffic with the hub.

The registration information and the bindings to IPoS internal addresses and encryption keys are stored in the IPoS management database containing parameters relevant for the operation and billing of users. These parameters are:

- Remote terminal serial number
- Customer name and contact information

Based on the parameters stored in the database, the hub creates the addresses and encryption keys for the different services to which the terminal is entitled. The IPoS internal addresses are configured in the terminal at installation time. The encryption keys are distributed to the remote terminals over the outroute carrier.

Several types of encryption keys are used in the IPoS system, as discussed in the security sections of this document. Key encrypting keys are used to encrypt other keys used to encrypt the actual user information. The remote terminal receives these keys during registration and stores the keys in the decryption hardware so that it is ready for decrypting the outroute information when entering the Active state.

After completing registration, the remote terminal is ready to begin operation in the IPoS system. This process is illustrated by figure 2.6.1.5-1.

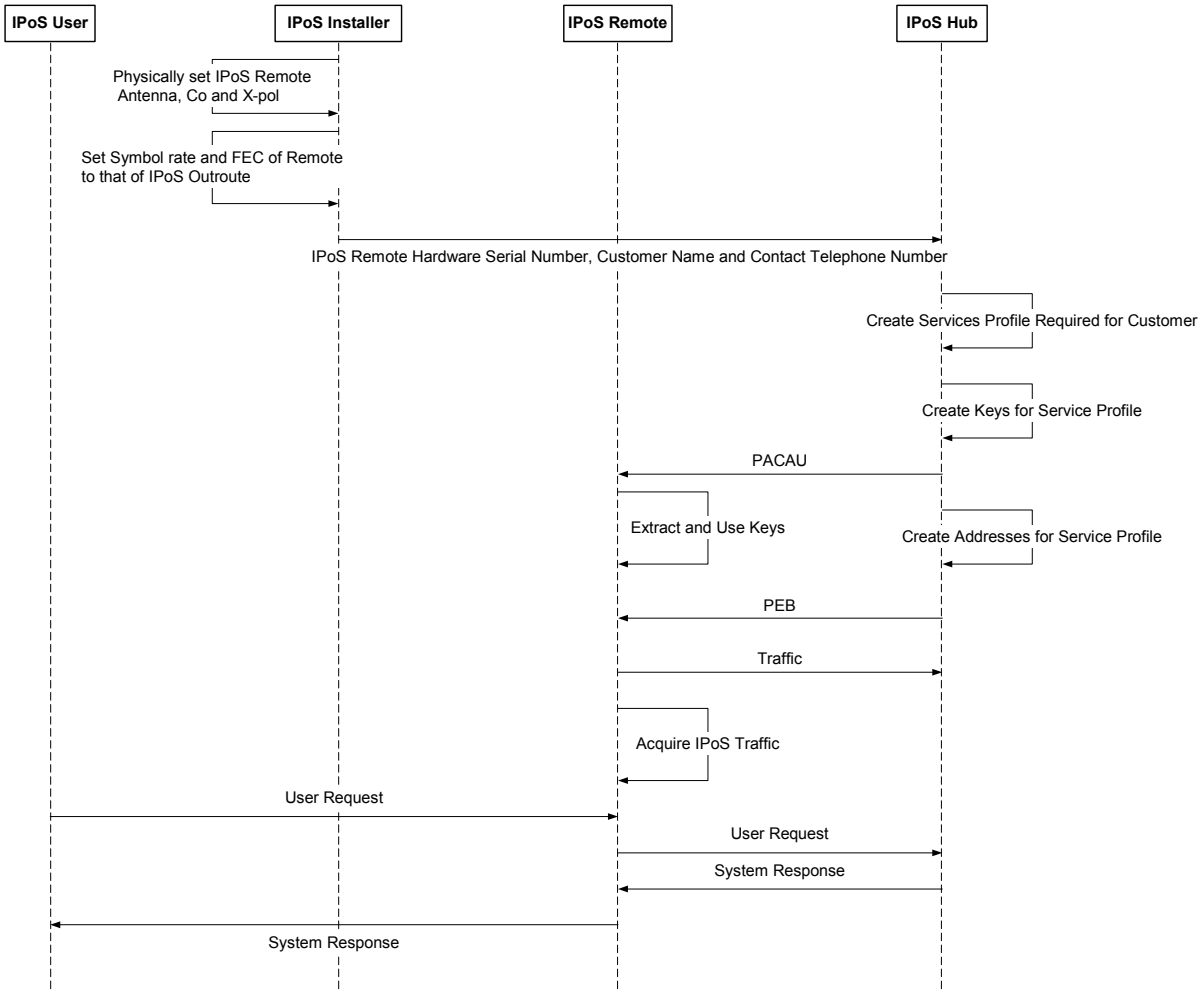


Figure 2.6.1.5-1. IPoS User Registration

2.6.1.6 Authentication

No terminal authentication procedure is required of the IPoS. The identity of a terminal is demonstrated by its ability to decrypt the messages received over the outroute containing the keys that will be used later to decrypt user information. For this action, the terminal Master Key (MK) installed at the terminals must coincide with an MK used at the hub to create the encryption keys. An unauthorized terminal will not have the same MK data as that on the authorized terminal, so it will not be able to decode outroute data.

2.6.2 Procedures in Idle Mode

The C-Plane provides the procedures that provide the bandwidth and support needed for the exchange of traffic between remote terminals and the hub.

2.6.2.1 System Information Reception

Before remote terminals can send information to the hub, they must gain knowledge of the inroute carrier frequencies used for user and control channels and the associated data rates and encoding used in these channels.

IPoS provides automated inroute load balancing and high availability by subdividing the IPoS inroutes into several inroute groups. The hub periodically broadcasts this information about the inroute groups over the outroute direction. The reception of the outroute carrier provides the remote terminals with system information related to the organization of the inroute into inroute groups, including the burst-time plan of all inroute groups associated with the IPoS outroute. The burst time plan provides the remotes with a description that includes:

- The inroute frequencies where the remote is allowed to transmit
- The duration and location of the bursts

The hub also advertises its traffic-loading levels in all inroute groups. The remote terminals use traffic-loading information to choose the least-loaded inroute group. However, the IPoS remote can change these inroute groups depending on the loading information conveyed by the Return Broadcast Channel, which is always monitored by the remote terminals to obtain the available inroute groups and the resources available in each inroute group. See figure 2.6.2.1-1.

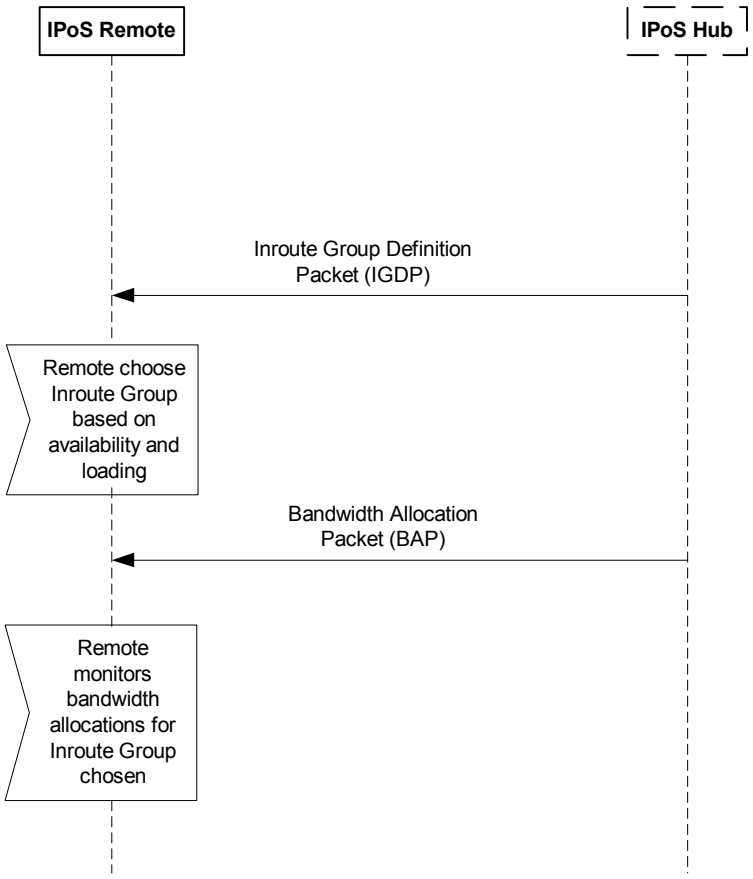


Figure 2.6.2.1-1. IPoS System Information Reception

Remote terminals monitor IGDP messages in all inroute groups simultaneously. When the remote terminals need to go active, the terminals choose a new inroute group based on their stored loading information. While active on the new inroute group, the remote terminals need to monitor for BAP messages in two inroute groups simultaneously, the new and the previous inroute group, until all BAPs have been received or lost. This technique also has the advantage that, should the inroute group fail, the IPoS remotes will sense the failure automatically (through information in the IGDP pertaining to the inroute group disappearing) and automatically switch to a new group.

2.6.2.2 Addressing and Routing

IPoS connectivity to the external terrestrial networks is based on IP version 4 (IPv4) routable addresses according to reference [3] (found in subsection 1.4 of this document) and will evolve to support IPv6 in reference [4] (found in subsection 1.4 of this document). The IPoS system is home to a static set of IP addresses that support both globally unique Internet addresses, or internal subnet IPoS addresses that are associated to a global hub address for each of the remote terminals. Network Address Translation (NAT) between the global IP and the internal subnet addresses is provided by the hub.

When the IPoS system allocates remote terminals, a static IP address is used as part of the commissioning process. This allocated IP address remains unchanged as long as the user is part of the IPoS system. The remote terminal's allocated IP address is the IP destination address used by hosts in the public network to contact the remote terminal in the IPoS system; IP packets received at the hub include this destination IP address that identifies the remote terminal to the hub. When an IPoS remote terminal intends to contact a host external to the IPoS system, the remote terminal includes the IP address of the destination host in the IP packets sent to the hub. The hub includes the IP destination address of the external host in the IP header of the packets sent by the hub over the terrestrial network so that they could be routed to the destination host.

When the remote terminal is using NAT, remote-terminal initiated connections are not possible until one of the globally unique Internet addresses supported by the hub is associated with the remote terminal as part of an Internet connection initiated by the hub.

IP addressing is not used for routing within IPoS. Instead, a layer 2 routing based on IPoS internal MAC addresses is used to identify and route within IPoS. The terminals' internal MAC addresses are created during terminal registration and the binding between the external IP address and its internal remote terminal MAC address is stored at the hub.

For IP packets arriving at the hub for delivery over the outroute direction, the hub performs the mapping between the remote terminal's IP address and the internal IPoS MAC address. The IP packet received at the hub, including the IP address for that particular terminal, is then encapsulated by the hub into PDUs that contain the internal MAC address used for routing within the IPoS system.

The internal MAC addressing provides three types of connectivity within the IPoS system:

1. PtP (point-to-point): defined with unicast addresses to deliver information from the hub to a single IPoS terminal.
2. PMP (point-to-multipoint): defined with multicast addresses to deliver the same information from the hub to a group of IPoS terminals.
3. Broadcast connectivity: defined with broadcast addresses to deliver the same information from the hub to all IPoS terminals in the system.

In the inroute direction, the remote terminals use the hub destination to send information over the inroute carriers. The remote terminals encapsulate the IP packets, including the IP address identifying the final destination to the Internet routers over the inroute direction. The hub removes the IPoS internal inroute encapsulation before sending the IP packet over the terrestrial Internet.

2.6.2.3 Access Session

IPoS provides satellite users with a virtual "always on" type of access that does not require the remote terminals to dial-up or establish an access session once the terminal has completed its registration. In this "always on" service, all registered

IPoS remote terminals maintain permanent IP connectivity to the external Internet, via the allocated IP address and internal IPoS connectivity and via the assigned MAC address, without the need for access session initiation or termination. The hub provides the attachment point where the IPoS network is connected to the Internet.

In Idle mode, the hub is always ready to accept IP packets for delivery to remote terminals over the IPoS system. For the remote terminals to be able to send IP packets, they first need to exchange control packets with the hub in order to obtain the inroute bandwidth needed to support the transmissions from the remote terminal to the hub.

The IPoS system is transparent to the service level sessions between user hosts and Internet servers that might take place based on the user IP address.

2.6.2.4 Bandwidth Request and Allocation

Before the remote terminal can transfer data over the inroute, it needs to request bandwidth on one of the inroute groups defined in the IPoS system. The Bandwidth Allocation Request (BAR) packet is sent by the remote over the Aloha channels defined for the particular inroute group.

The hub processes the bandwidth request and acknowledges the bandwidth request with an explicit acknowledgment sent over the multicast logical channel associated to the particular inroute group.

Once the hub determines the bandwidth to be assigned over the particular inroute group, it sends the remote terminal the Bandwidth Allocation Packet (BAP) indicating the assigned timeslots in the inroute group. After the remote terminal transmits the assigned timeslots, the hub indicates which bursts were received correctly. Bandwidth allocation is illustrated in figure 2.6.2.4-1.

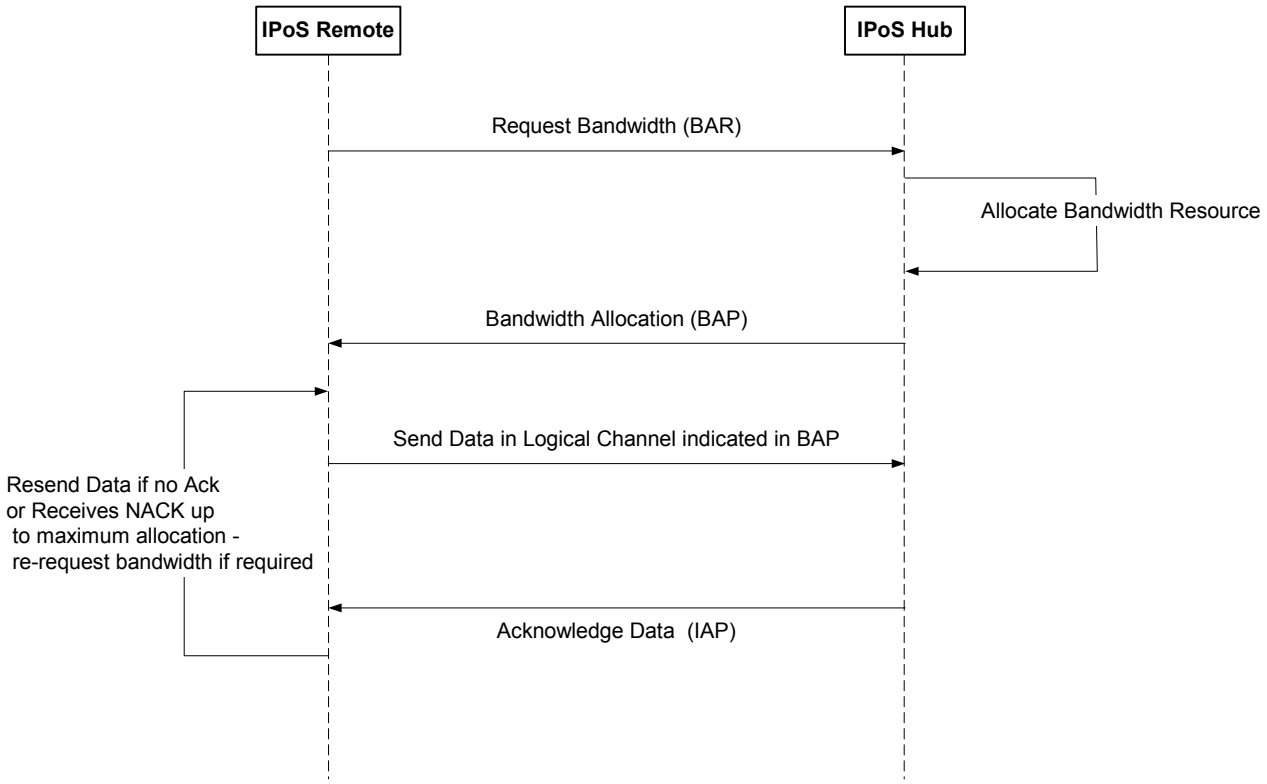


Figure 2.6.2.4-1. Bandwidth Request Allocation

2.6.2.5 Transition to the Idle State

The remote terminal transitions to the Idle state when it completes its transmission and does not receive a bandwidth assignment after a bandwidth request. (The transition of remote terminals to the Idle state is controlled by the hub; a mobile terminal needs to transmit when it receives a bandwidth assignment even if it has not data to transmit.) From the Idle state, the remote terminal will send a new bandwidth request to resume sending data on the inroute.

2.6.3 Transport Procedures

The following subsections describe the procedures for the reliable transfer of user, control, and management information between remote terminals and the hub. This reliable transfer of information in the IPoS system is based on:

- Encapsulation formats specific for each information type
- The segmentation used to break the information into fragments that can be accommodated within the length limits of the different encapsulation formats
- The definition of logical channels that convey preestablished message types

- The error protection, error detection, and error control procedures used over the different types of logical channels.

Internet user traffic (e.g., TCP applications) originating at the remote terminal passes through the IPoS system in the following steps:

- The PC sends IP packets to the IRU in the remote terminal.
- The IRU segments, encapsulates, and transmits each IP packet (possibly in multiple bursts) over the inroute carriers.
- The hub reassembles each IP packet from burst received from the remote terminal.
- The hub communicates with the destination host over the Internet using the destination address in the received packet.
- Packets received from the destination host are buffered at the hub then sent to the remote terminal over the outroute carrier.

2.6.3.1 Encapsulation Formats

The processes in the peer layers at the remote terminal and the hub interact with each other through the set formats designated as PDUs. These PDUs contain the set of user, control, and management information exchanged across the air interface in the form described in this standard, where PDUs are defined for the physical layer, PHY PDU; at the MAC sublayer, MAC PDU; and at the SLC sublayer, SLC PDU.

These exchanges of PDUs among the different peer layers are illustrated in figure 2.6.3.1-1.

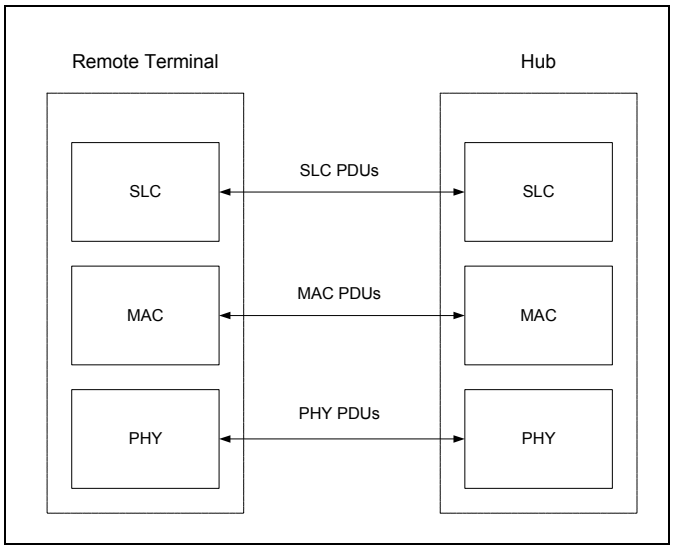


Figure 2.6.3.1-1. Peer Layer PDU Exchanges

2.6.3.2 Segmentation and Packetization

The encapsulation formats transferred across the IPoS system are referred to as PDUs.

In general, the format of the PDUs used across IPoS peer layers consists of a header, the payload or Service Data Unit (SDU), and a trailer. Headers, SDUs, and trailers are defined specifically for each layer.

Primitives across the sublayer, SAPs, provide the information and the instruction for different sublayers in IPoS protocol. The information from the higher layer PDUs is encapsulated into the SDU of the lower sublayers, including a DVB-MPEG compatible protocol encapsulation used in the multiplexer sublayer that allows multiple types of services to share the same outroute PHY. Figure 2.6.3.2-1 illustrates the different encapsulation formats used in the IPoS outroute direction.

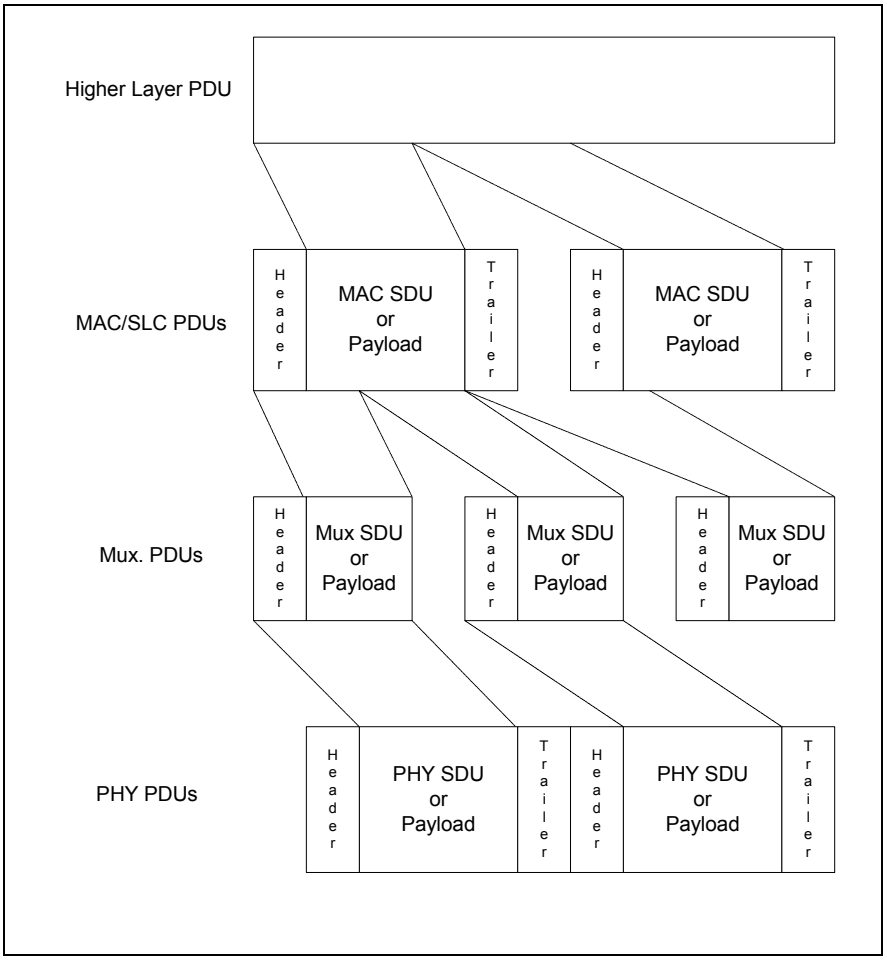


Figure 2.6.3.2-1. IPoS Outroute Data Flows

Figure 2.6.3.2-2 illustrates the encapsulation formats across the inroute, formats that are similar to the formats in the outroute without the multiplexing layer.

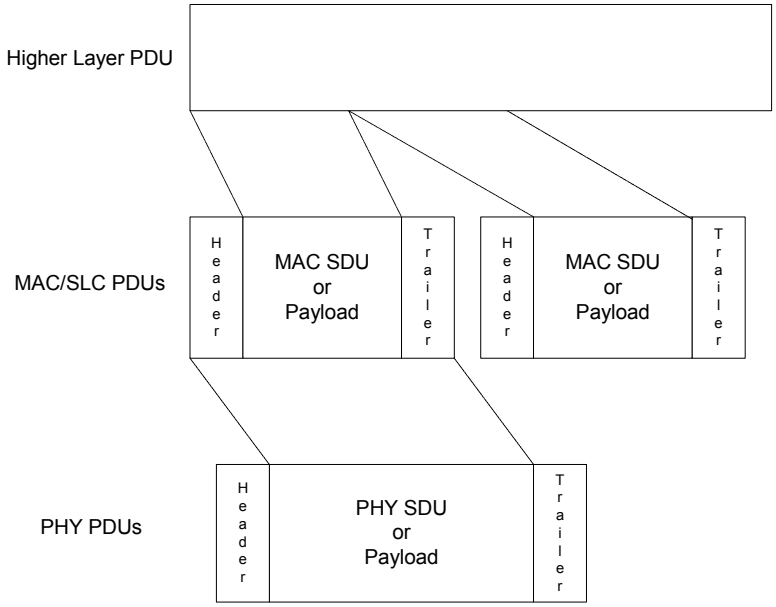


Figure 2.6.3.2-2. IPoS Inroute Data Flows

2.6.3.3 Logical Channels

Transfers of user, control, and management information in IPoS take place over logical channels. Logical channels are unidirectional and defined in both the outroute and inroute directions.

Outroute logical channels are classified according to the characteristics of the information transferred into

- Traffic channels: used for transferring user plane and management plane information
- Control channels: used for transferring control plane information

Also, outroute logical channels are classified by the type of connectivity provided from the IPoS hub to the IPoS remotes. Three types of connectivity are supported by the outroute logical channels:

1. PtP connections: defined with a unicast address to deliver information to a single IPoS terminal
2. PMP connections: defined with a multicast address to deliver the same information to a group of IPoS terminals
3. Broadcast connectivity: delivers the same information to all IPoS terminals in the system

In the inroute direction, IPoS provides PtP connectivity only from the particular remote terminal to the hub, both for traffic and control channels. The classification of logical channels for the inroute direction is made according to whether the channel bandwidth could be shared by multiple remote terminals or

is dedicated to a particular terminal. Two types of inroute logical channels are defined in the IPoS:

1. Unallocated channels: These are channels shared by multiple IPoS terminals using contention access procedure.
2. Allocated channels: These are channels dedicated to one specific IPoS terminal for the transmission of user information during an allocated time interval.

The designation of traffic channels and their connectivity is shown in figure 2.6.3.3-1. Also, unallocated channels could be used to carry user traffic.

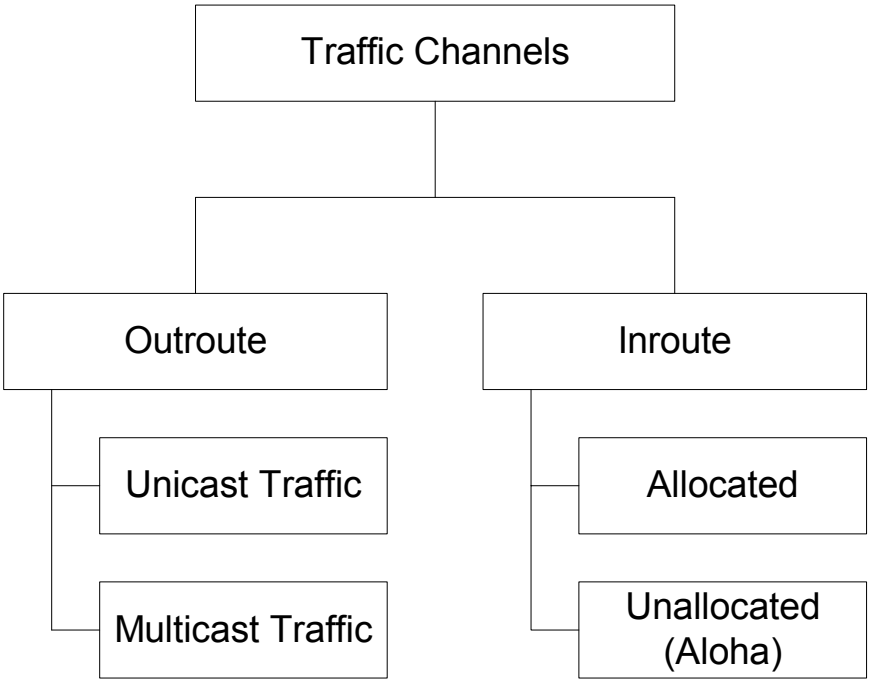


Figure 2.6.3.3-1. Traffic Channel Types

Figure 2.6.3.3-2 shows the different types of logical control channels defined both for both outroute and inroute directions.

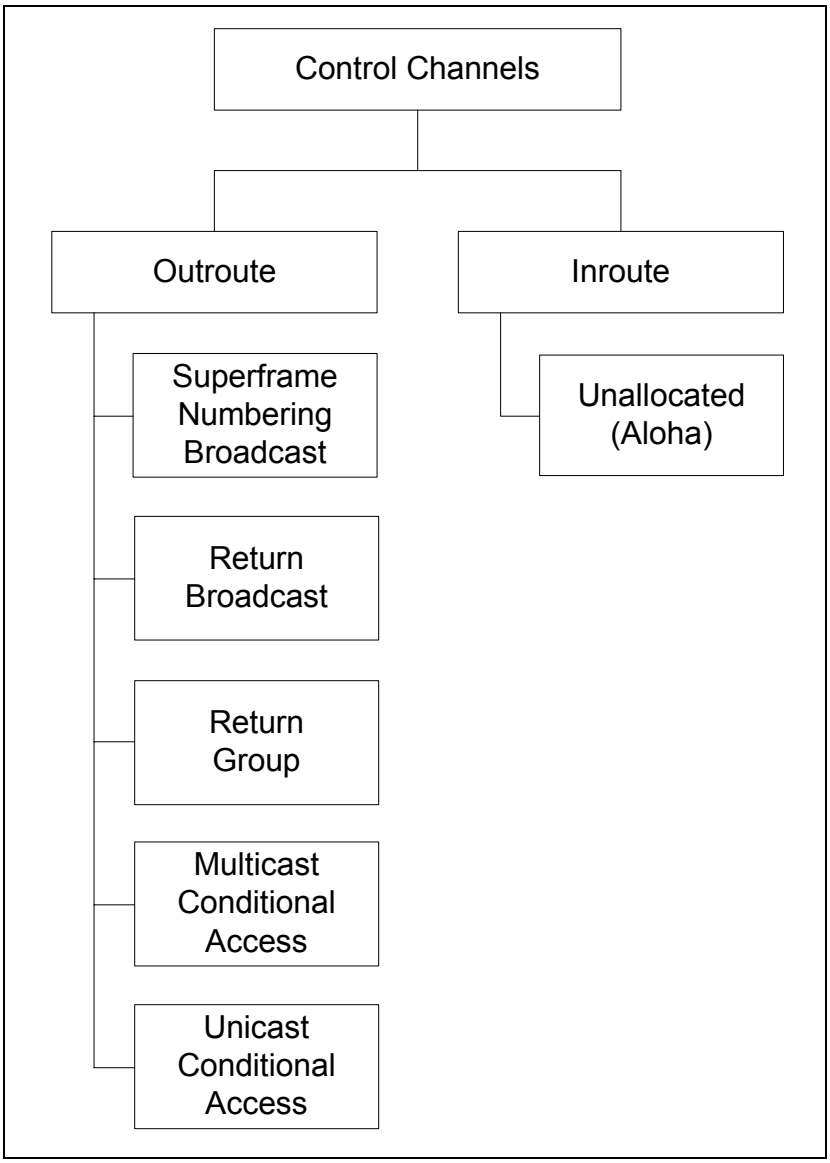


Figure 2.6.3.3-2. Control Channel Types

2.6.3.4 Error Control

In IPoS, error control is achieved by a combination of error control strategies across the different layers of the protocol stack. These strategies include:

- FEC in the physical sublayer
- Cyclic Redundancy Checking (CRC) in the MAC sublayer
- Procedures to control the repetition of SLC/MAC segments

The FEC design in IPoS is different for outroute and inroute directions:

- The outroute direction uses the concatenation of a Reed-Solomon code with a convolutional code.
- The inroute direction includes the option to use convolutional or Turbo coding.

The IPoS procedures that control repetitions over the different logical channels include three modes of operation:

1. Unacknowledged operation
2. Acknowledged operation
3. Contention access

2.6.3.4.1 Unacknowledged Operations

Unacknowledged operation is applicable to all logical channels in the outroute direction and for all addressing modes: broadcast, multicast, and unicast. In this unacknowledged operation, the MAC PDUs are neither acknowledged nor retransmitted, even if transmission errors or format errors are detected.

2.6.3.4.2 Acknowledged Operation

IPoS provides acknowledged operation over the inroute traffic, allocated, and logical channels. Acknowledged operation uses an Automatic Request (ARQ) procedure providing error correction by retransmission for the recovery of remote terminal transmissions that have been corrupted.

The ARQ procedure allows selective repeat retransmission where only those inroute bursts that are not acknowledged by the hub in the outroute direction (the acknowledgment could also be lost) will be retransmitted by the remote terminal. ARQ go-back-N-based procedure is also supported by this standard.

Error detection at the hub and the remote terminals are based on CRC fields included at the MAC sublayer.

2.6.3.4.3 Contention Access

Contention access based on a backoff-and-retry procedure is used on the unallocated inroute channels to arbitrate the access of multiple remote terminals to these inroute logical channels. These inroute unallocated logical channels are also designated as Aloha channels. The contention procedure provides the ability to transmit the same information on two unallocated channels in a scheme designated as diversity Aloha, which reduces the overall probability of collision.

The Aloha channels are primarily used for control messages, mainly bandwidth requests from the remote terminals, in the inroute direction. Piggybacking of user data with control messages is also supported in the Aloha channels.

3 IPoS PHYSICAL LAYER

3.1 Introduction

This section specifies the PHY portion of the air interface between the IPoS remotes and IPoS hub. The requirements provide for the interoperation of IPoS remote terminals, made by different manufacturers, with the IPoS hub.

3.2 Physical Layer Overview

The Physical Layer function will provide the physical data transfer methods to the data link and higher layers. At the PHY, IPoS makes no distinction between the transport methods provided for C-Plane and U-Plane. This distinction is made at higher layers.

The IPoS PHY is based upon a configuration in which the two directions of transmission are highly asymmetric. This PHY consists of:

- Outroute transmissions from the IPoS hub to user terminals, which are forward broadband satellite channels with transmission formats specified for Digital Video Broadcast (DVB-S) by the European Broadcasting Union (EBU) and were originally intended for the broadcasting of digital television via satellite.

- Inroute transmissions from the remote terminals to the IPoS hub are point-to-point, narrowband return channels, either using bandwidth assigned by the gateway to individual remote terminals or using bandwidth shared by all terminals on a contention basis.

The services and functions that are provided by the PHY are grouped into the following subsections for their description:

- The Radio Frequency (RF) parameters, bands, bandwidths, and power levels.

- The outroute baseband processing including the modulation, coding, and scrambling of the transport streams of fixed length packets.

- The inroute baseband processing of U-Plane, C-Plane, and M-Plane inroute information flows.

- The performance of local measurements such as received E_{bt}/N_o, recovered clock and status, and supervision of the physical parameters (such as timing) and their reporting to higher layers.

Figure 3.2-1 illustrates the PHY at the IPoS remote and its relationship to the MAC sublayer.

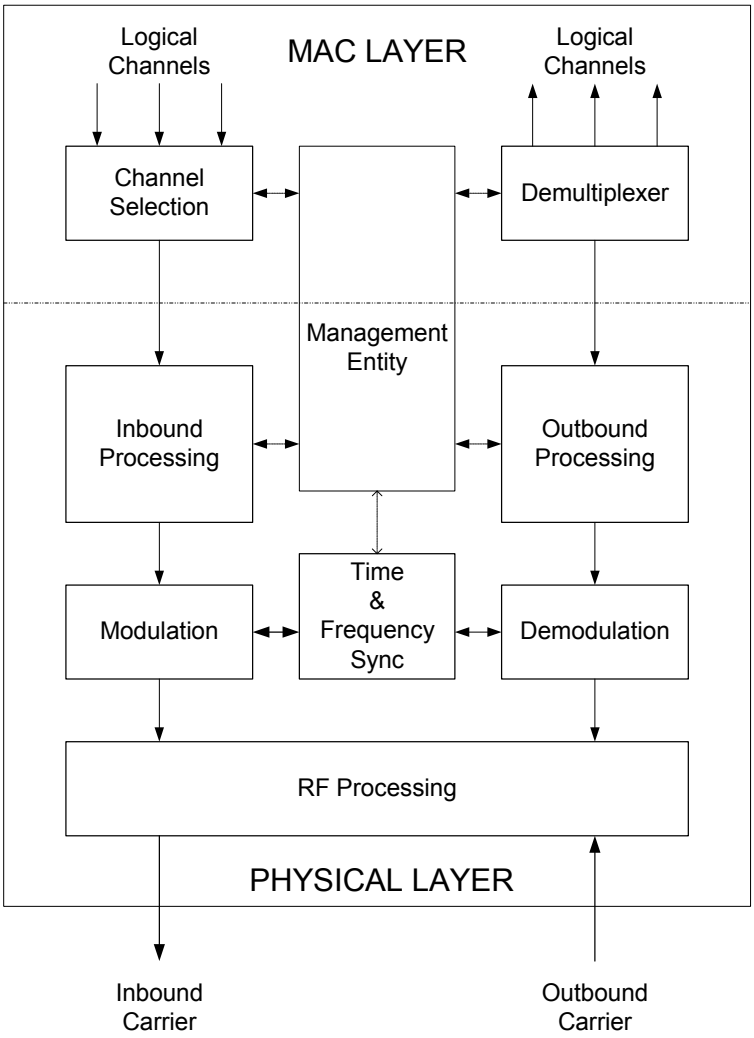


Figure 3.2-1. The Physical Layer and Its Relationship to the MAC Layer

3.3 Radio Transmission

This subsection defines the radio parameters of the RF channels used in the IPoS system. In particular it addresses:

- Frequency bands
- Channelization
- Transmit power levels
- Out-of-band emissions
- Phase noise
- Antenna characteristics

3.3.1 Operating Bands

The IPoS PHY interfaces provide bidirectional satellite links using commercial satellites with spectrum allocated to fixed satellite service (FSS). The spectrum allocation might vary with the geographical region and economic considerations. This IPoS standard only provides radio parameters for Ku-band operation.

In North America, the spectrum allocation at Ku-band is divided into two equal 500 MHz bands as follows:

- The band from 14.00 GHz to 14.5 GHz shall be used by the IPoS remote and IPoS hub to transmit (uplink) in Earth-to-Space direction.
- The band from 11.7 GHz to 12.2 GHz shall be used by the IPoS remote and IPoS hub to receive (downlink) in the Space-to-Earth direction.

In Europe the spectrum allocated to FSS spectrum at Ku-band consists of two 250 MHz in the following bands:

- The band from 14.00 GHz to 14.25 GHz shall be used by the IPoS remote and IPoS hub to transmit (uplink).
- The band from 12.5 GHz to 12.75 GHz shall be used by the IPoS remote and IPoS hub to receive (downlink).

The following European shared bands for FSS and terrestrial fixed services could also be used:

- The band from 14.25 GHz to 14.50 GHz shall be used by the IPoS remote and IPoS hub to transmit (uplink).
- The band from 10.7 GHz to 11.7 GHz shall be used by the IPoS remote and IPoS hub to receive (downlink).

The spectrum allocations in India and other parts of Asia are:

- The band from 14.00 GHz to 14.5 GHz shall be used by the IPoS remote and IPoS hub to transmit (uplink).
- The band from 12.2 GHz to 12.75 GHz shall be used by the IPoS remote and IPoS hub to receive (downlink).

To support domestic and international markets at Ku-band, the IPoS remote and IPoS hub shall be capable of:

- Transmitting from 13.75 to 14.50 GHz
- Receiving from 10.7 GHz to 12.7 GHz

3.3.2 Duplexing Methods

The 500 MHz band from 14.00 to 14.50 GHz is used by the transmissions from the hub, commonly called the outroute carrier, and the transmissions from the IPoS remotes, commonly known as the inroute carrier. In the case of North America's commercial satellites, the carriers are amplified, downconverted, and retransmitted over the corresponding subband in the 11.7 to 12.2 GHz band. These geostationary earth orbit (GEO) satellites have a 2-degree minimum orbital spacing, and their transponders possess a 36 MHz nominal bandwidth within a 40 MHz transponder spacing.

IPoS can operate on transponders of up to 54 MHz bandwidth. IPoS can also operate on a single transponder that is subdivided in frequency to one or more services. The IPoS inroute transmits in one of several narrowband carriers amplified by a transponder using a different subband.

3.3.3 RF Channel Spacing

The RF nominal bandwidth of the modulated carriers is a function of the symbol rate and the modulation characteristics for the particular carrier. The channel spacing for the outroute and inroute carriers should be adequate to support the nominal bandwidths given in the following subsections.

The IPoS remote shall support symbol rates of 1 to 45 Msps on the IPoS outroute.

Nominal channel bandwidths required for some typical IPoS outroute symbol rates are illustrated in table 3.3.3-1.

Table 3.3.3-1. Outroute Channel Spacing for Sample Symbol Rates

Symbol Rate (Msps)	Minimum Channel Spacing (MHz)
1.25	1.5
2.5	3.0
5.0	6.0
10.0	12.0
20.0	24.0
30.0	36.0
45.0	54.0

3.3.4 Inroute Nominal Bandwidth

The remote unit shall be capable of transmitting at 64, 128, and 256 ksps. The minimum RF bandwidth for the inroute carriers is given in table 3.3.4-1.

Table 3.3.4-1. Inroute Channel Spacing for Sample Symbol Rates

Symbol Rate (ksps)	Minimum Channel Spacing (kHz)
64	80
128	160
256	320

The minimum inroute carrier spacing shall be 1.25 times the symbol rate.

3.3.5 Frequency Tuning

The transmit and receive carriers shall be programmable in 100 Hz increments across the full transmit, 14.00 to 14.50 GHz, and receive 10.70 to 12.70 GHz bands, starting with the lower frequency in the band.

3.3.6 Frequency Stability

The frequency stability of the transmitted inroute carrier shall be accomplished by locking the IPoS remote frequency reference with the symbol clock frequency of the outroute carrier. The frequency stability of the reference used for the outroute carrier symbol clock generation shall be better than 3×10^{-9}.

3.3.6.1 Frequency Accuracy

The frequency accuracy of the transmit inroute carrier shall be better than 1×10^{-8}.

To protect users from RF transmissions, the IPoS remote's transmitter shall not transmit unless both the outroute carrier and the frame timing are acquired during the intended transmitted burst.

3.3.7 Output Power

The IPoS remote's ODU shall provide a nominal output power level as given in table 3.3.7-1 (into a 1.3:1 load voltage standing wave ratio (VSWR)). The output power is referenced to the output at the antenna feedhorn interface. FCC and European Radio Communication Committee rules, which allow power levels up to a 33 dBm ODU, are also acceptable with license exception. Where operational circumstances allow, ODU powers of less than 30 dBm shall be used.

Table 3.3.7-1. Output Power Requirement

@ Room Temperature	-40 °C to +55 °C
+30.0 dBm ±1.0 dB	+30.0 dBm ±1.5 dB

3.3.8 Output Power Control

Output power control shall be implemented. The accuracy of the power control shall meet the specification in table 3.3.8-1.

Table 3.3.8-1. Output Power Control Requirement

Desired Power Level	Output Power @ Room Temperature		
(% Backoff From Full Power)		1/2 Watt (Nominal)	1 Watt (Nominal)
0%	$P_{0\%}$ =	+27.0 dBm ±1.0 dB	+30.0 dBm ±1.0 dB
25%	$P_{25\%}$ =	$P_{0\%}$ – 3 dB ±1.5 dB	$P_{0\%}$ – 3 dB ±1.5 dB
50%	$P_{50\%}$ =	$P_{25\%}$ – 3 dB ±1.5 dB	$P_{25\%}$ – 3 dB ±1.5 dB

3.3.9 EIRP

In the U.S.A., the antenna beamwidth must be 2˚ or less. Outside the U.S.A., a beamwidth of 3˚ or less is required. Table 3.3.9-1 shows typical antenna sizes and effective isotropic radiated power (EIRP), assuming a 30 dBm amplifier.

Table 3.3.9-1. Typical EIRPs

Antenna Diameter (Meters)	EIRP (dBW) 14.25 GHz
0.65	38.0
0.74	39.1
0.98	41.6
1.2	43.3
1.8	46.8

3.3.10 Off-Axis EIRP Spectral Densities

The off-axis spectral density (copolar and cross-polar) transmitted within the 14.00 to 14.50 GHz band on the geostationary plane under clear sky conditions shall not exceed the following values:

$15 – 39 \log_{10} (\theta)$ dBW/4 kHz for $1° <= \theta <= 7°$

-6.0 dBW/4 kHz for $7° < \theta <= 9.2°$

$18 – 39 \log_{10} (\theta)$ dBW/ 4 kHz for $9.2° < \theta <= 48°$

-24 dBW/4 kHz for $48° < \theta <= 180°$.

where:

Theta (θ) is the angle in degrees from the axis of the main lobe.

3.3.11 Carrier on EIRP

In the Transmission Enable state, the IPoS remote's EIRP shall not exceed 4 dBW in any 4 kHz band within the 14.00 to 14.50 GHz band.

3.3.12 Unwanted Emissions

Unwanted emissions are classified in two domains:

- The emissions outside the nominal bandwidth of the transmission in 14.00 to 14.50 GHz.
- Spurious emissions or emissions outside the 14.00 to 14.50 GHz band.

3.3.13 In-Band Unwanted Emissions

3.3.13.1 Carrier-on State

The spectral density of unwanted emissions outside the nominated bandwidth shall not exceed 4 dBW in any 100 kHz band within 14.00 GHz and 14.50 GHz.

3.3.13.2 Carrier-off State

In the Transmission Disable state, the spectral density of unwanted emissions outside the nominated bandwidth shall not exceed -21 dBW in any 100 kHz within 14.00 GHz and 14.50 GHz.

3.3.13.3 Off-Axis Spurious Emissions

The following specifications apply to earth terminals transmitting at EIRP values up to and including $EIRP_{max}$:

- The earth terminal shall not exceed the limits for radiated interference field strength over the frequency range from 30 MHz to 1 GHz, as specified in table 3.3.13.3-1.

Table 3.3.13.3-1. Limits of Radiated Field Strength at a Test Distance of 10 Meters in a 100 kHz Bandwidth

Frequency Range MHz	Quasi-Peak Limits dBµV/m
30 MHz to 230 MHz	30
230 MHz to 1000 MHz	37

The lower limits shall apply at the transition frequency.

- When the IPoS remote is in the Transmission Disabled state, the off-axis spurious radiation from the earth terminal in any 100 kHz band shall not

exceed the limits given in table 3.3.13.3-2 for all off-axis angles greater than 7 degrees.

Table 3.3.13.3-2. Limits of Spurious Field Strength Transmission Disabled State

Frequency band	EIRP limit (dBpW)
1.0 GHz–10.7 GHz	48
10.7 GHz–21.2 GHz	54
21.2 GHz–40 GHz	60

The lower limits shall apply at the transition frequency.

- This specification applies outside the nominated bandwidth for earth terminals. For both the Carrier-on and Carrier-off states, the off-axis spurious radiation from the earth terminal appearing in any 100 kHz band from the earth terminal shall not exceed the limits shown in table 3.3.13.3-3, for all off-axis angles greater than 7 degrees.

Table 3.3.13.3-3. Limits of Spurious Transmissions

Frequency Band	EIRP Limit (dBpW)
1.0 GHz to 3.4 GHz	49
3.4 GHz to 10.7 GHz	55
10.7 GHz to 13.75 GHz	61
13.75 GHz to 14.00 GHz	95 (Note 1)
14.50 GHz to 14.75 GHz	95 (Note 1)
14.75 GHz to 21.2 GHz	61
21.2 GHz to 40.0 GHz	67
Note: This limit may be exceeded in a frequency band that shall not exceed 50 MHz, centered on the carrier frequency, provided that the on-axis EIRP density, measured in 100 kHz at the frequency of the considered spurious, is 50 dB below the maximum on-axis EIRP density of the signal (within the nominated bandwidth) expressed in dBW/100 kHz.	

3.3.14 Antenna

The nominal IPoS terminal antenna is a 74 cm elliptical antenna (98 cm x 56 cm) satisfying the requirements in the following subsections. Other antenna sizes might be used to provide adequate performance under strict propagation environments or lower performing satellite transponders as long as they meet the requirements in the following subsections.

3.3.14.1 Antenna Polarization

Ku-band transponders use linear polarization, either horizontally or vertically, but not simultaneously. The IPoS remote shall be able to use the same polarization for transmit and receive, and this polarization shall be adjustable to match the satellite polarization within all locations in the coverage area, e.g., CONUS in North America.

3.3.15 Copolar Antenna Sidelobes

The copolar sidelobe pattern of the antenna in the plane of the geostationary satellite orbit as it appears at a particular earth station location shall conform to the more stringent North American limits:

In the plane of the geostationary satellite orbit as it appears at the particular earth station location:

$29–25 \log_{10} (\theta)$ dBi	for $1° <= \theta <= 7°$
+8 dBi	for $7° < \theta <= 9.2°$
$32–25 \log_{10} (\theta)$ dBi	for $9.2° < \theta <= 48°$
-10 dBi	for $48° < \theta <= 180°$

where:

θ is the angle in degrees from the axis of the main lobe.

dBi refers to dB relative to an isotropic radiator.

The peak gain of any individual sidelobe or the copolar plane of the geostationary plane may not exceed the envelope defined above for θ between 1.0 and 7.0 degrees. For θ greater than 7.0 degrees, the envelope may be exceeded by no more than 10% of the sidelobes, provided no individual sidelobe exceeds the gain envelope given above by more than 3 dB.

In all other directions outside the geostationary plane, or in the plane of the horizon including any out-of-plane potential terrestrial interference paths, the copolar gain of the antenna outside the main beam shall lie below the envelope defined by:

$32–25 \log_{10} (\theta)$ dBi	for $1° <= \theta <= 48°$
-10 dBi	for $48° < \theta <= 180°$

where:

θ and dBi are defined above.

For the purposes of copolar sidelobes outside the main beam, the envelope may be exceeded by no more than 10% of the sidelobes provided no individual

sidelobe exceeds the gain envelope given above by more than 6 dB. The region of the main reflector spillover energy is to be interpreted as a single lobe and shall not exceed the envelope by more than 6 dB.

3.3.16 Cross-Polar Antenna Sidelobes

The off-axis, cross-polarization gain of any antenna to be employed in transmission from an earth station to a space station in the domestic fixed-satellite service shall be defined by:

$19 - 25 \log_{10} (\theta)$ dBi for $1.8° < \theta <= 7°$

-2 dBi for $7° < \theta <= 9.2°$

where

θ and dBi are defined above.

3.3.16.1 Receiver G/T

For the IPoS remote, the minimum antenna gain-to-noise temperature (G/T) when operating in a clear sky condition shall be 15 dB/K.

3.3.17 Phase Noise Specifications

The integrated phase noise, as measured at the IPoS remote's output, shall be less than 4 degrees rms when integrated from 1 kHz to 128 kHz. The phase noise of the inroute carrier shall not exceed the mask in table 3.3.17-1.

Table 3.3.17-1. Suggested IPoS Reference Source Phase Noise

Offset Frequency	Phase Noise
Up to 1 kHz	<-69 dBc/Hz
10 kHz	<-59 dBc/Hz
100 kHz	<-81 dBc/Hz
128 kHz	<-82 dBc/Hz
550 kHz	<-83 dBc/Hz
1 MHz	<-87 dBc/Hz
>10 MHz	<-122 dBc/Hz

3.3.18 Illustrative Example Link Budgets

Figure 3.3.18-1 gives the forward carrier link budget, and figure 3.3.18-2 gives the return carrier link budget.

31-Oct-02 FORWARD CARRIER LINK BUDGET
01:51 PM Satellite: W1-D4

0.5 dB mispoint 0.74m equivalent diameter 0.98m x 0.57m elliptical

	BASELINE PARAMETERS	Value	Unit
CARRIER DATA	No of Crrs/Xponder	1	
	Carrier Info Rate	55294	Kbps
	FEC Code Rate	0.667	
	R/S Codec Rate	0.922	
	Crr Symbol Rate	45000	Ksps
	Min Reqd Ebi/No	5.4	dB
	No of bits/symbol	2.0	Bits
	Demod BT Product	1.2	
	Crr Noise Bandwith	54000	KHz
SATELLITE DATA	Satellite	W1-D4	
	Location	350.0	WL
	EIRP Contour at Direc PC	49.4	dBW
	G/T Contour at Hub	4.00	dB/K
	Attn Setting	0.0	dB
	Xponder Gain	184.2	dB
	SFD	-90.00	dBW/m2
	Xponder Bandwidth	54.0	MHz
	Agg Input BO	1.0	dB
	Agg Output BO	0.5	dB
	Uplink Frequency	13.840	GHz
	Dnlink Frequency	11.540	GHz
GROUND SEGMENT DATA	Tx Antenna Dia	7.2	meters
	Tx Antenna Gain	57.9	dBi
	Tx Pointing Losses	0.7	dB
	Equivalent Rx Antenna Dia	0.74	meters
	Rx Antenna Gain	37.3	dBi
	Rx Pointing Losses	0.5	dB
	Pre LNA Losses	0.4	dB
	LNA Noise Temp	68	K
	Ant,etc Temp	46.0	K
	Cl Sky Noise Temp	135.5	K
	Rx Clr Sky G/T	15.58	dB/K
RAIN MARGINS	Uplink Rain Attn	0.1	dB
	Dnlink Rain Attn	0.1	dB
	Up Fade Pwr Cntrl	0.0	dB
SITE GEOGRAPHIC DATA	Tx E/S Location	Frankfurt	
	Tx E/S Latitude	50.0	N
	Tx E/S Longitude	8.5	E
	Tx E/S Elev Angle	30	deg
	Rx E/S Location	London	
	Rx E/S Elev Angle	30.1	deg
XPOL ISOLATION DATA	S/C Isolation	33.0	dB
	Tx E/S Isolation	35.0	dB
	Rx E/S Isolation	20.0	dB
MISC LOSSES	Uplink Free Sp Loss	207.0	dB
	Dnlink Free Sp Loss	205.4	dB
	Uplink Atmos Attn	0.3	dB
	Dnlink Atmos Attn	0.2	dB

	SUMMARY				
	% Avail S/C Power Reqd/Crr		100.00		%
	Downlink Fade Margin		2.2		dB
	Clear Sky Link Margin		2.3		dB
	LINK PERFORMANCE	Cl Sky	Up Fade	Dn Fade	Unit
UPLINK BUDGET	Satellite SFD	-90.0	-90.0	-90.0	dBW/m2
	Input Backoff	1.0	1.1	1.0	dB
	Crr Flux Density	-91.0	-91.1	-91.0	dBW/m2
	Gain of a Sq meter	44.3	44.3	44.3	dBi
	Uplink Path Losses	207.3	207.4	207.3	dB
	Carrier Up EIRP	72.0	72.0	72.0	dBW
	Satellite G/T	4.0	4.0	4.0	dB/K
	C/N Uplink	20.0	19.9	20.0	dB
DOWNLINK BUDGET	EIRP Contour	49.4	49.4	49.4	dBW
	Output Backoff	0.5	0.5	0.5	dB
	Carrier Dn EIRP	48.9	48.9	48.9	dBW
	Dnlink Path Losses	205.6	205.6	205.7	dB
	Rx Pointing Losses	0.5	0.5	0.5	dB
	Cl Sky E/S G/T	15.6	15.6	15.6	dB/K
	Degradation in G/T	0.0	0.0	0.16	dB
	C/N Downlink	9.6	9.6	9.4	dB
COMPOSITE LINK	C/N Uplink	20.0	19.9	20.0	dB
	C/N Downlink	9.6	9.6	9.4	dB
	C/I Dnlink Adj Transponder	20.0	20.0	20.0	dB
	C/I Uplink Adj Sat	27.0	26.9	27.0	dB
	C/I Dnlink Adj Sat	17.7	17.7	17.7	dB
	C/I Xpol	17.8	17.8	17.8	dB
	C/(Nu,d)	9.2	9.2	9.0	dB
	C/(Nu,d,ims/c)	8.9	8.9	8.7	dB
	C/(Nu,d,im,i)Total	7.8	7.8	7.7	dB
	LINK MARGIN	2.3	2.3	2.2	dB
MODEM	Minimum Reqd Ebi/No		5.4	dB	
	Minimum Reqd Ebt/No		3.3	dB	
	10*log(Rbt/Noise BW)		2.2	dB	
	Minimum Reqd C/N		5.5	dB	
EARTH STATION HPA	E/S EIRP/Crr Reqd (Cl Sky)		72.0	dBW	

Figure 3.3.18-1. Illustrative Example IPoS Outroute Link Budget (Forward)

RETURN CARRIER LINK BUDGET

Satellite: W1-F2

BASELINE PARAMETERS	Value	Unit
No of Crrs/Xponder	400	
Carrier Info Rate	128	Kbps
FEC Code Rate	0.500	
R/S Codec Rate	1.000	
Crr Xmission Rate	256	Kbps
Min Reqd Ebi/No	3.2	dB
No of bits/symbol	2.0	Bits
Demod BT Product	1.2	
Crr Noise Bandwith	154	KHz
Carrier Spacing	180	KHz
Satellite	W1-F2	
Location	350.0	WL
EIRP Contour at Hub	49.0	dBW
G/T Contour at Remote	3.60	dB/K
Attn Setting	6.0	dB
Xponder Gain	186.7	dB
SFD	-89.6	dBW/m2
Xponder Bandwidth	72.0	MHz
Agg Input BO	8.0	dB
AIBO/AOBO Difference	4.3	dB
Uplink Frequency	14.042	GHz
Dnlink Frequency	12.542	GHz
Tx Antenna Dia	0.74	meters
Tx Antenna Gain	39.0	dBi
Tx Pointing Losses	0.5	dB
Equivalent Rx Antenna Dia	7.20	meters
Rx Antenna Gain	57.5	dBi
Rx Pointing Losses	0.5	dB
Pre LNA Losses	0.2	dB
LNA Noise Temp	100	K
Ant,etc Temp	39.0	K
Cl Sky Noise Temp	150.3	K
Rx Clr Sky G/T	35.5	dB/K
Uplink Rain Attn	6.6	dB
Dnlink Rain Attn	0.1	dB
Up Fade Pwr Cntrl	0.0	dB
Tx E/S Location	Lisbon	
Tx E/S Elev Angle	40.9	deg
Rx E/S Location	Frankfurt	
Rx E/S Latitude	49.8	N
Rx E/S Longitude	351.4	W
Rx E/S Elev Angle	32.9	deg
S/C Isolation	33.0	dB
Tx E/S Isolation	25.0	dB
Rx E/S Isolation	35.0	dB
Uplnk Free Sp Loss	206.9	dB
Dnlnk Free Sp Loss	206.1	dB
Uplink Atmos Attn	0.3	dB
Dnlink Atmos Attn	0.2	dB

	SUMMARY				
	% Xponder Bandwidth Reqd/Crr			0.25	%
	Clear Sky Link Margin			5.0	dB
	LINK PERFORMANCE	Cl Sky	Up Fade	Dn Fade	Unit
	Satellite SFD	-89.6	-89.6	-89.6	dBW/m2
	Input Backoff	35.7	42.3	35.7	dB
	Crr Flux Density	-125.3	-131.9	-125.3	dBW/m2
UPLINK	Gain of a Sq meter	44.4	44.4	44.4	dBi
BUDGET	Uplink Path Losses	207.2	213.8	207.2	dB
	Carrier Up EIRP	37.5	37.5	37.5	dBW
	Satellite G/T	3.6	3.6	3.6	dB/K
	C/N Uplink	10.6	4.0	10.6	dB
	EIRP at the Hub	49.0	49.0	49.0	dBW
	Output Backoff	31.4	38.0	31.4	dB
	Carrier Dn EIRP	17.6	11.0	17.6	dBW
DOWNLINK	Dnlink Path Losses	206.3	206.3	206.4	dB
BUDGET	Rx Pointing Losses	0.5	0.5	0.5	dB
	Cl Sky E/S G/T	35.5	35.5	35.5	dB/K
	Degradation in G/T	0.0	0.0	0.15	dB
	C/N Downlink	23.1	16.5	22.8	dB
	C/N Uplink	10.6	4.0	10.6	dB
	C/N Downlink	23.1	16.5	22.8	dB
	C/I Transponder Intermodulation	13.3	6.7	13.3	dB
	C/I Uplink Adj Sat	14.8	8.2	14.8	dB
COMPOSITE	C/I Dnlink Adj Sat	37.9	31.3	37.9	dB
LINK	C/I Xpol	21.1	15.9	21.1	dB
	C/(Nu,d)	10.4	3.8	10.4	dB
	C/(Nu,d,ims/c)	8.6	2.0	8.6	dB
	C/(Nu,d,im,i)Total	7.5	0.9	7.5	dB
	LINK MARGIN	5.0	-1.5	5.0	dB
	Minimum Reqd Ebi/No		3.2	dB	
MODEM	Minimum Reqd Ebt/No		0.2	dB	
	10*log(Rbt/Noise BW)		2.2	dB	
	Minimum Reqd C/N		2.4	dB	
	E/S EIRP/Crr Reqd (Cl Sky)		37.5	dBW	
	Tx Gain - Pointing Loss		38.5	dB	
EARTH	TRIA and other losses		1.0	dB	
STATION					
HPA					
	Composite HPA Backoff		0.0	dB	
	Minimum HPA Power Rating		1.00	watts	

Figure 3.3.18-2. Illustrative Example IPoS Inroute Link Budget (Return)

3.4 Outroute Physical Layer

The IPoS outroute PHY uses DVB modulation that is compatible with reference [7] (found in subsection 1.4 of this document). The high-level structure of the remote IPoS outroute PHY is illustrated by figure 3.4-1.

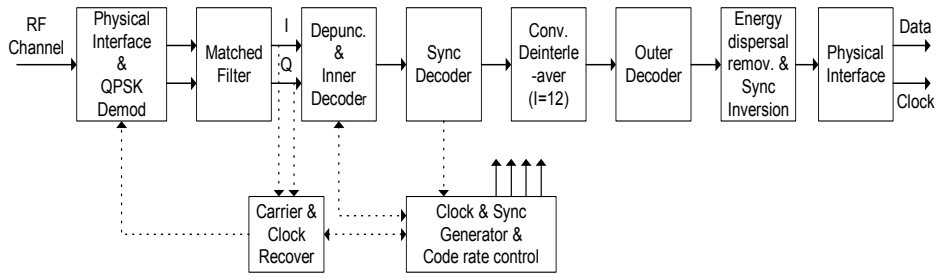


Figure 3.4-1. IPoS Outroute High-Level Functional Structure

The following paragraphs describe the blocks illustrated by figure 3.4-1 and are extracted from reference [7] (found in subsection 1.4 of this document):

- **IF interface and QPSK demodulator**: This unit performs the quadrature-coherent demodulation function and the analog-to-digital conversion providing "soft decision" I and Q information to the inner decoder.

- **Matched filter**: This unit performs the complementary pulse shaping filtering of raised cosine type according to the rolloff. The use of a Finite Impulse Response (FIR) digital filter could provide equalization of the channel linear distortions in the Integrated Receiver Decoder (IRD).

- **Carrier/clock recovery unit**: This device recovers demodulator synchronization. The probability of slip generation over the full carrier to noise (C/N) range of the demodulator should be very low.

- **Clock and Sync Generator Code Rate Control**: This unit provides clock and synchronization information for the other functional blocks of the decoder.

- **Inner decoder**: This unit performs first-level error protection decoding. This unit will try each of the code rates and puncturing configurations until lock is acquired. Furthermore, it is in a position to resolve $\pi/2$ demodulation phase ambiguity.

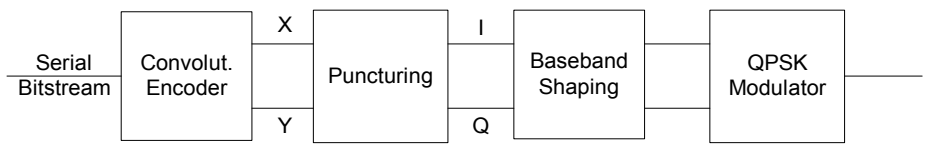
- **Sync byte decoder**: By decoding the MPEG-2 (figure 3.4-1) sync bytes, this decoder provides synchronization information for deinterleaving. It is also in a position to recover π ambiguity of QPSK demodulator (not detectable by the Viterbi decoder).

- **Convolutional deinterleaver**: This device allows the error bursts at the output of the inner decoder to be randomized on a byte basis in order to improve the burst error correction capability of the outer decoder.

- **Outer decoder**: This unit provides second-level error protection.
- **Energy dispersal removal**: This unit recovers user data by removing the randomizing pattern used for energy dispersal purposes and changes the inverted sync byte to its normal MPEG-2 sync byte value.
- **Baseband physical interface**: This unit adapts the data structure to the format and protocol required by the external interface.

3.4.1 Modulation QPSK

The system shall employ conventional gray-coded QPSK modulation with absolute mapping (no differential coding). Bit mapping in the signal space, as given on figure 3.4.1-1, shall be used.



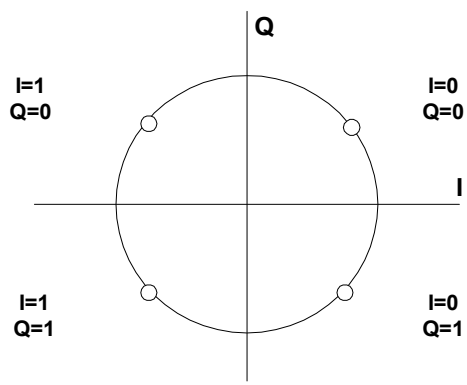


Figure 3.4.1-1. QPSK Constellation

Prior to modulation, the I and Q signals (mathematically represented by a succession of Dirac delta functions spaced by the symbol duration Ts = 1/Rs, with appropriate sign) shall be square root raised cosine filtered.

3.4.1.1 Pulse Shaping

The baseband square root raised cosine filter shall have a theoretical function defined by the following expressions:

$$H(f) = 1 \qquad \text{for } |f| < f_N(1-\alpha)$$

$$H(f) = \left\{ \frac{1}{2} + \frac{1}{2} \sin \frac{\pi}{2 f_N} \left[\frac{f_N - |f|}{\alpha} \right] \right\}^{\frac{1}{2}} \quad \text{for } f_N(1-\alpha) \le |f| \le f_N(1+\alpha)$$

$$H(f) = 0 \qquad \text{for } |f| > f_N(1-\alpha)$$

where:

$$f_N = \frac{1}{2T_s} = \frac{R_s}{2} \text{ is the Nyquist frequency}$$

α is the rolloff factor. For the outroute, the rolloff factor α shall be 35%.

3.4.2 Frame Structure

The outroute signal is organized as a time division multiplex composed of fixed length MPEG-2 transport packets.

The total length of each MPEG transport packet is 188 bytes. This includes a sync word byte (i.e., 47_{HEX} or binary 01000111). The transmission order starts from the most significant bit (MSB) at the left (i.e., 0) of the sync word byte. See figure 3.4.2-1.

Figure 3.4.2-1. MPEG-2 Transport Mux Packet

The outroute frame consists of eight MPEG transport packets. The sync word byte of the first MPEG transport packet is inverted bit-wise (i.e., $B8_{HEX}$) to aid with the frame synchronization functions. The frame structure is shown in figure 3.4.2-2.

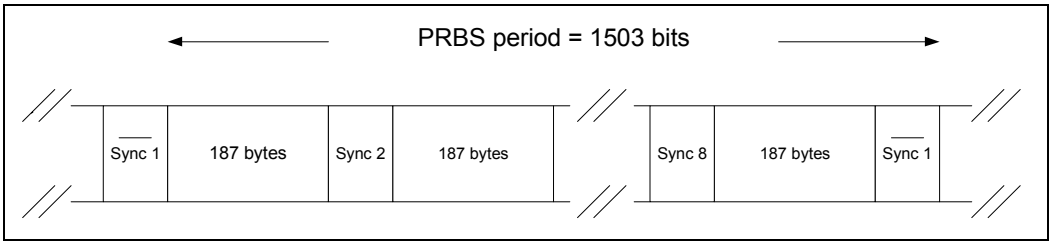


Figure 3.4.2-2. Outroute Frame: Sync Bytes and Randomization Sequence R

The outroute frame consists of 1504 bytes. The first byte is the inverted sync word byte followed by 1053 bytes designated as a pseudorandom binary sequence (PRBS) period.

3.4.3 Scrambling

To ensure adequate binary transitions, the outroute frame shall be randomized in accordance with the configuration in figure 3.4.3-1.

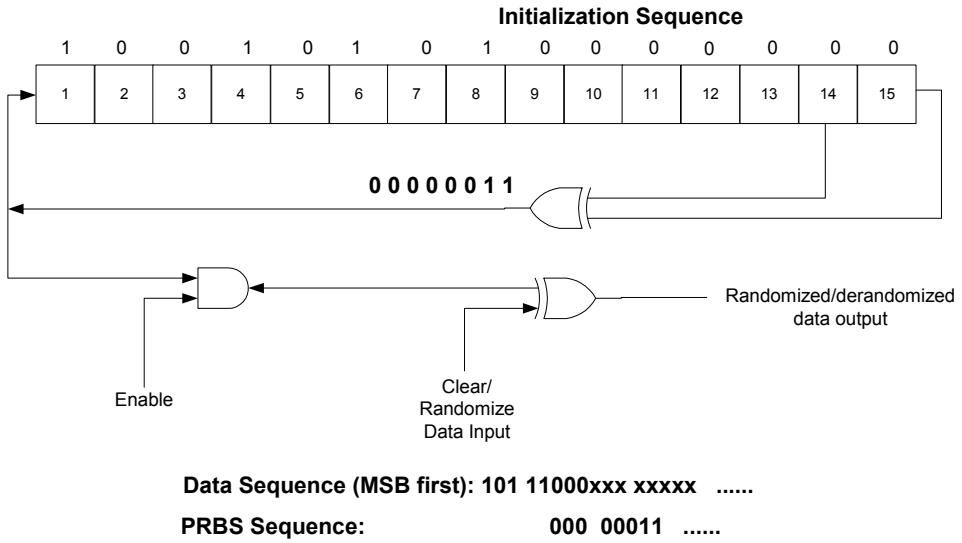


Figure 3.4.3-1. Descrambler Diagram

The polynomial for the PRBS generator shall be:

$$1 + x^{14} + x^{15}$$

To provide an initialization signal for the descrambler, the MPEG-2 sync byte of the first transport packet in a group of eight packets is bit-wise inverted from 47_{HEX} to $B8_{HEX}$. This process is referred to as the "Transport Multiplex Adaptation."

As indicated in figure 3.4.3-1, loading of the initialization sequence, 100101010000000, into the PRBS generator, shall be done at the start of every frame. The first bit at the output of the PRBS generator shall be applied to the first bit (i.e., MSB) of the first byte following the inverted MPEG-2 sync bytes of the first packet in the frame. Thus the period of the PRBS sequence is 1,503 bytes.

3.4.4 Channel Coding

3.4.4.1 Reed-Solomon (RS) Coding

The coding shall be as defined in reference [7] (found in subsection 1.4 of this document). This specification is reiterated here and illustrated in figure 3.4.4.1-1.

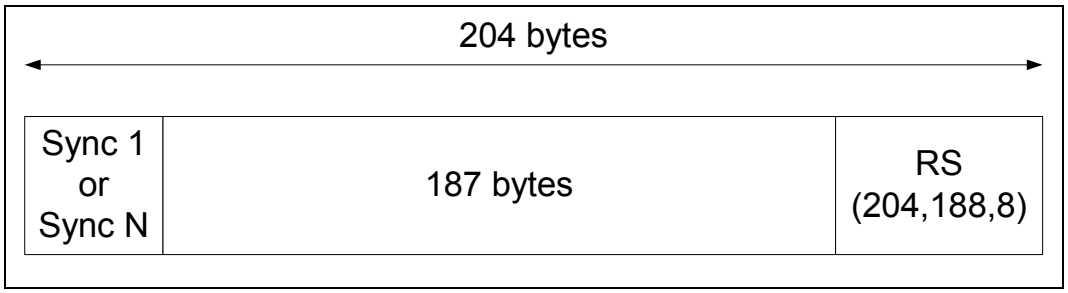


Figure 3.4.4.1-1. Reed-Solomon (204,188, T=8) Error Protected Packet

RS (204,188, T = 8) shortened code from the original RS (255,239, T = 8) code, shall be applied to each randomized transport packet (188 bytes) to generate an error-protected packet (see figure 3.4.4.1-1 and figure 3.4.4.1-2). RS coding shall also be applied to the packet sync byte, either noninverted (i.e., 47_{HEX}) or inverted (i.e., $B8_{HEX}$).

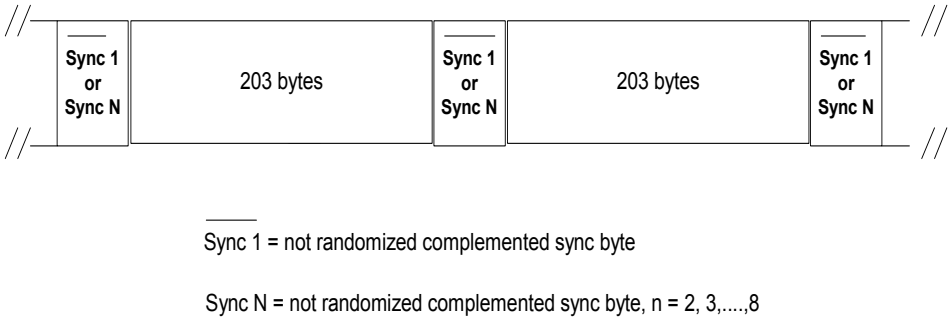


Figure 3.4.4.1-2. Interleaved Frames; Interleaving Depth I = 12

The code generator polynomial of the RS code is:

$$g(x) = (x + \lambda^0)(x + \lambda^1)(x + \lambda^2)....(x + \lambda^{15})$$

where $\lambda = 02_{HEX}$

The field generator polynomial is:

$$p(x) = x^8 + x^4 + x^3 + x^2 + 1$$

The shortened RS code may be implemented by adding 51 bytes, all set to zero, before the information bytes at the input of a (255,239) encoder. After the RS coding procedure, these null bytes shall be discarded.

3.4.4.2 Convolutional Coding

The system shall allow for a range of punctured convolutional codes, based on a Rate 1/2 convolutional code with constraint length K = 7 and generator polynomial $(171, 133)_{HEX}$. This will allow selection of the most appropriate level of error correction for a given service or data rate. The system shall allow to

obtain convolutional coding with code Rates of 1/2, 2/3, 3/4, 5/6, and 7/8 by puncturing the output of the basic Rate 1/2 convolutional code.

The puncturing patterns given in table 3.4.4.2-1 shall be used (see also figure 3.4.1-1).

Table 3.4.4.2-1. Punctured Code Definition

Code Rate	Puncture Pattern
1/2	X: 1 Y: 1
2/3	X: 1 0 Y: 1 1
3/4	X: 1 0 1 Y: 1 1 0
5/6	X: 1 0 1 0 1 Y: 1 1 0 1 0
6/7	X: 1 0 0 1 0 1 Y: 1 1 1 0 1 0
7/8	X: 1 0 0 0 1 0 1 Y: 1 1 1 1 0 1 0

Note: At the receiver, each of the code rates and puncturing configurations is in a position to be tried until lock is acquired. The demodulator is able to resolve 180 degrees phase ambiguity by decoding the MPEG-2 sync byte delimiting the interleaved frame.

3.4.4.3 Deinterleaving

The convolutional deinterleaving process shall be based on reference [8] (found in subsection 1.4 of this document), the compatible Ramsey type III/Forney approach, with I = 12. The interleaved frame shall be composed of overlapping error-protected packets and shall be delimited by inverted or non-inverted MPEG-2 sync bytes as defined in Reference [1], subsection 2.4.3.2.

The deinterleaver may be composed of I = 12 branches, cyclically connected to the input byte stream by the input switch. Each branch shall be a first-in, first-out (FIFO) shift register, with depth (M j) cells (where M = 17 and j = branch index, with branch index 0 providing the largest delay). The FIFO cells shall contain 1 byte, and the input and output switches shall be synchronized.

For synchronization purposes, the sync bytes and the inverted sync bytes always shall be routed in branch index 12 of the interleaver (corresponding to a null delay).

3.4.4.4 Receiver Demodulation Performance

The unit shall meet or exceed the BER vs. E_{bi}/N_o requirements defined in Reference [7] (found in subsection 1.4 of this document), which are repeated in table 3.4.4.4-1.

Table 3.4.4.4-1. Receiver Demodulator Performance Requirements (Including Implementation Losses)

Inner FEC Code Rate	Threshold E_{bi}/N_o (dB) @ BER = $2x10^{-4}$ (Viterbi Decoder Output), QEF[2] After Reed-Solomon (dB)	
	IF	RF
1/2	4.5	4.9
2/3	5	5.4
3/4	5.5	5.9
5/6	6	6.4
7/8	6.4	6.8

3.5 Inroute Physical Layer

The high-level structure of the inroute transmit chain is shown in figure 3.5-1.

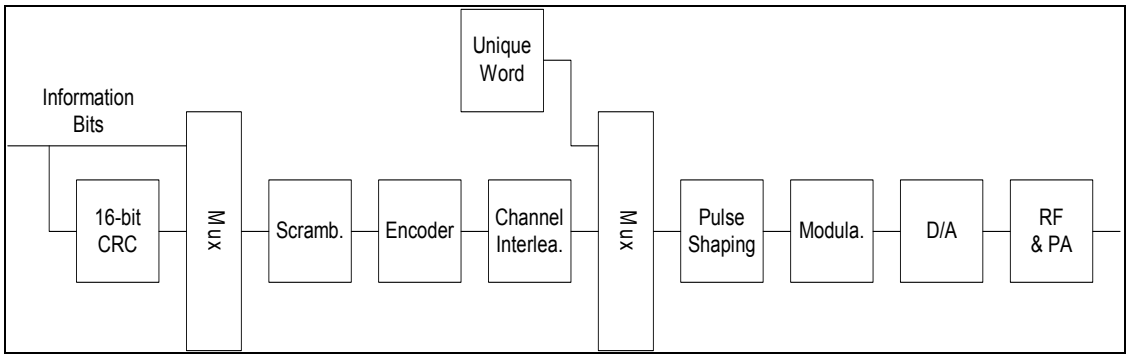


Figure 3.5-1. High-Level IPoS Inroute Diagram

The following paragraphs describe the blocks illustrated in figure 3.5-1.

- **16-bit CRC**: This unit adds bits to the information stream to allow the verification of its integrity across the inroute direction.
- **Scrambler**: This unit randomizes the inroute stream to avoid the concentration of transmitted energy in particular parts of the spectrum.
- **Encoder**: This unit introduces an error protection bit using convolutional or Turbo-coding techniques
- **Channel Interleaver**: This unit modifies the order of the transmitted bits in an attempt to randomize the errors introduced in the inroute channel.
- **Unique Word (UW)**: This unit introduces fixed patterns of bits to assist with the timing synchronization of the received signal.

[2] Quasi-error-free (QEF) means less than one uncorrected error event per hour, corresponding to BER = 10^{-10} to 10^{-11} at the input of the MPEG-2 demultiplexer.

- **Pulse shaping**: This unit conforms to the spectrum of the transmitted signal.
- **Modulator**: This unit maps the baseband bits into the constellation of allowed carrier phases.
- **D/A (digital-to-analog) converter**: This unit transforms the digital samples of the inroute waveform into an analog signal.
- **RF and PA (power amplifier)**: This unit performs the frequency translation and amplification of the inroute signal

3.5.1 Modulation

The IPoS remote shall use Constant Envelope Offset-QPSK (CE-OQPSK) modulation for the IPoS inroute. The baseband equivalent diagram of the modulator is shown in figure 3.5.1-1.

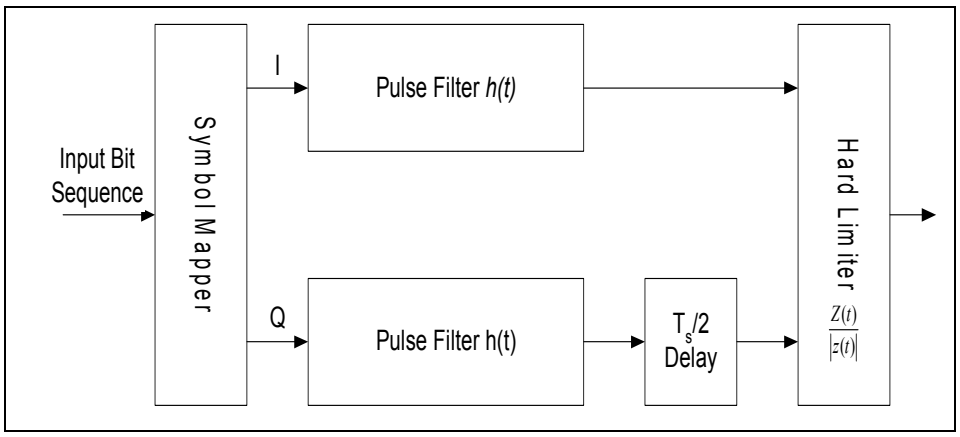


Figure 3.5.1-1. Block Diagram of the Modulator

The OQPSK baseband signal before the hard limiter is given by:

$$z(t) = \sum_k \{I(k) \cdot h(t - kT_s) + j \cdot Q(k) \cdot h(t - kT_s - T_s / 2)\}$$

where:

$I(k) + j \cdot Q(k)$ denotes QPSK symbol.

T_S is the symbol duration.

$h(t)$ is the shaping pulse created by the shaping filter.

k is the time index.

The mapping between the input bit sequence to the modulator and the OQPSK symbol is given in table 3.5.1-1.

Table 3.5.1-1. OQPSK Signal Mapping

Bit Pair (b(2k-1),b(2k))	Modulated Symbol (I(k) + j Q(k))
(1, 1)	$(1+j)/\sqrt{2}$
(0, 1)	$(-1+j)/\sqrt{2}$
(0, 0)	$(-1-j)/\sqrt{2}$
(1, 0)	$(1-j)/\sqrt{2}$

3.5.1.1 Pulse Shaping

The baseband square root raised cosine filter shall have a theoretical function defined by the following expression:

$$H(f) = 1 \qquad \text{for } |f| < f_N(1-\alpha)$$

$$H(f) = \left\{ \frac{1}{2} + \frac{1}{2}\sin\frac{\pi}{2f_N}\left[\frac{f_N - |f|}{\alpha}\right] \right\}^{\frac{1}{2}} \qquad \text{for } f_N(1-\alpha) \le |f| \le f_N(1+\alpha)$$

$$H(f) = 0 \qquad \text{for } |f| > f_N(1-\alpha)$$

where:

$f_N = \dfrac{1}{2T_s} = \dfrac{R_s}{2}$ is the Nyquist frequency

α is the rolloff factor. For the inroute, the rolloff factor α shall be 40%.

3.5.1.2 Constant Envelope OQPSK

The representation of the CE-OQPSK-modulated RF carrier after the hard limiter is:

$$s(t) = \text{Real}\left\{ \sqrt{P}\,\frac{z(t)}{|z(t)|}\exp(j2\pi f_c t + \phi(t)) \right\}$$

3.5.2 Unique Words

The UW used for inroutes with convolutional coding at 64 ksps and 128 ksps inroutes and for inroutes with Turbo coding at 128 ksps and 256 ksps are the following:

In-phase: 1000 0110 1100 0101 0110 1111

Quadrature: 1010 1100 1100 0110 1101 1100

The UW used for 256 ksps convolutionally coded inroutes are the following:

In-phase: 0101 0100 1110 0111

Quadrature: 1010 0110 1100 0000

The left-most bit of the UWs is transmitted first.

3.5.3 Coding

Two types of encoding schemes could be used in the inroute direction:

1. Convolutional encoding, where data is passed through the CRC encoder, followed by the scrambler and convolutional encoder
2. Turbo encoding (optional), where data is passed through the CRC encoder, followed by the scrambler, Turbo encoder, and channel interleaver

In either case, the maximum (uncoded) burst size will be 768 bytes (6144 bits).

3.5.3.1 Convolutional Coding

The unit shall use Rate ½ sequential FEC encoding. A block diagram of the convolutional coder is illustrated by figure 3.5.3.1-1.

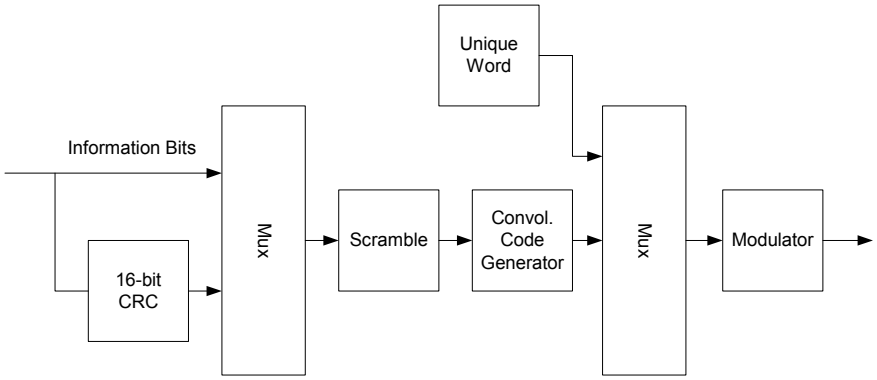


Figure 3.5.3.1-1. Convolutional Coder Block Diagram

3.5.3.1.1 Cyclical Redundancy Check

Each packet is protected by a 16-bit CRC. The highest bit of the MSB shall be sent out first when the scrambler requires the CRC value. Other aspects of the hardware CRC generator are:

- CRC-CCITT generator polynomial:

  $$g(x) = x^{16} + x^{12} + x^5 + 1$$

- The state of all registers shall be set to one at the beginning of each packet.

- While all systematic bits shall be transmitted without inversion, the checksum bits shall be inverted prior to transmission.

The data format entering the sequential coder is illustrated by figure 3.5.3.1.1-1.

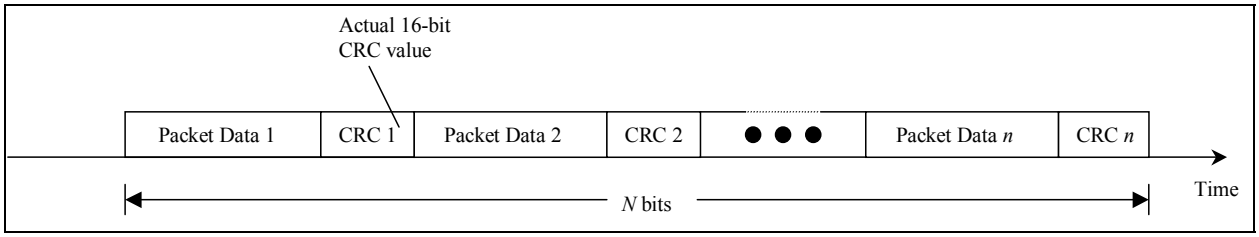


Figure 3.5.3.1.1-1. Data Format Entering Scrambler

3.5.3.1.2 Data Scrambler

A CCITT v.35 data scrambler shall be implemented. The scrambler shall have odd parity. The scrambler shall not perform any differential encoding. The scrambler shall be reset at the beginning of every burst.

For convolutional coding, the adverse state counter in the CCITT v.35 standard is modified as follows:

- The adverse state counter shall be initialized to zero at the commencement of each burst within any frame.

- The adverse state detector considers each input along with the 8th earlier transmitted bit relative to the input bit. An adverse state is when the input bit and the 8th earlier transmitted bit are the same for a number of consecutive bits of data. This number is 30 in the V.35 standard but 31 in the IPoS variation of V.35 used with convolutional coding.

Also, at the beginning of each burst within any frame, it shall be assumed that all previous transmitted bits were, in order of the earliest to the latest time, 11111111111111111110.

3.5.3.1.3 Convolutional Code Generator

The convolutional encoder is Rate ½, K = 36 with two generator polynomials: G1 and G2. The code is systematic, where G1 is the identity matrix. The G2 matrix represents the formation of parity bits from a serial shift register encoder. The G2 connection matrix is specified in table 3.5.2.1.2-1; it can be read as a

shift register XOR connection map where 1 = connect and 0 = no connect. See table 3.5.3.1.3-1.

Table 3.5.3.1.3-1. Convolutional Encoder G2 Matrix

X	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
G(x)	1	1	1	0	0	1	1	0	0	1	0	0	1	1	0	0	0	1	1	1	0	0	1	0	1	0	1	0	1	1	0	0	1	0	1	1

3.5.3.2 Turbo Coding (Optional)

The unit may implement a Turbo encoder. Where Turbo coding is used, a channel interleaver shall also be used. A block diagram of this encoder is illustrated by figure 3.5.3.2-1.

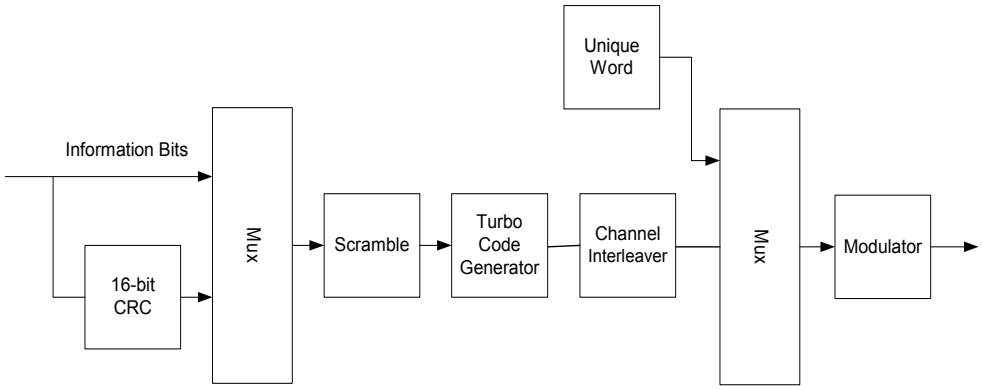


Figure 3.5.3.2-1. IPoS Turbo Coder Block Diagram

3.5.3.2.1 Cyclical Redundancy Check

The Turbo coder shall use the same CRC as the convolutional encoder. This is specified in subsection 3.5.3.1.1.

3.5.3.2.2 Data Scrambler

The Turbo coder shall use the CCITT v.35 data scrambler without the modifications defined in subsection 3.5.3.1.2.

3.5.3.2.3 Turbo Generator

The unit shall implement a Turbo encoder that uses a parsed parallel-concatenated convolutional code (P2C3). See figure 3.5.3.2.3-1.

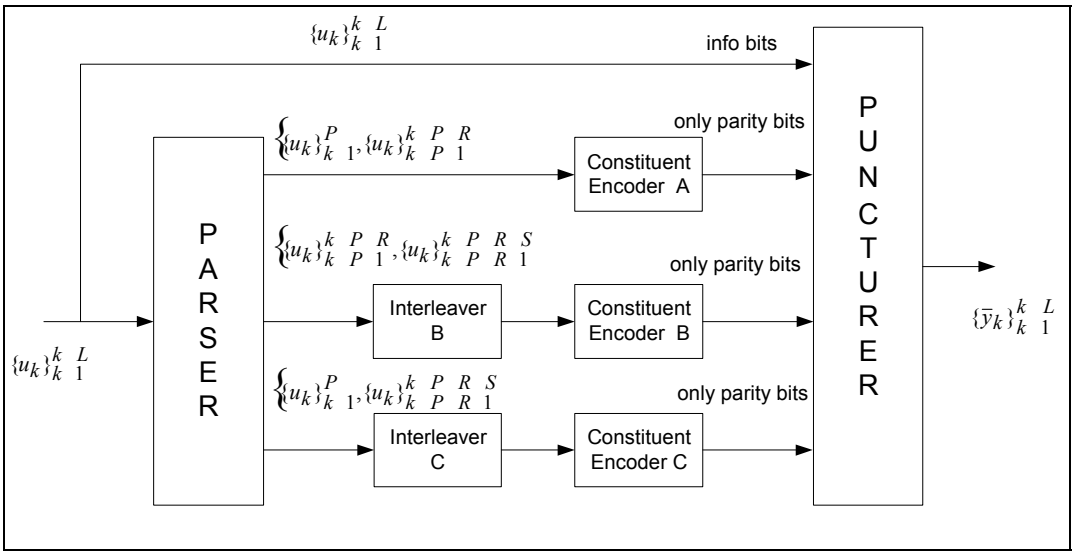


Figure 3.5.3.2.3-1. Encoder Block Diagram for Parsed Parallel Concatenated Convolutional Codes

This is a Rate 1/2 systematic, recursive, convolutional code where the parity bit and next state equations are given in the following subsections.

3.5.3.2.3.1 Parser

Each constituent encoder processes approximately two-thirds of an L information bit. Information bits in a burst, $\{u_k\}_{k=1}^{k=L}$, are divided into three subgroups: the first P bits $\{u_k\}_{k=1}^{P}$, the following R bits $\{u_k\}_{k=P+1}^{k=P+R}$, and the last S bits $\{u_k\}_{k=P+R+1}^{k=P+R+S}$. The values P, R, and S are determined as follows:

$$\begin{cases} \text{if } (L \bmod 3) = 0, \text{ then, } P = R = S = L/3 \\ \text{if } (L \bmod 3) = 1, \text{ then, } P = (L-1)/3+1, R = S = (L-1)/3 \\ \text{if } (L \bmod 3) = 2, \text{ then, } P = R = (L-2)/3+1, S = (L-2)/3 \end{cases}$$

Note that currently the burst payload size shall be restricted to an integer number of bytes, hence, P, R, and S all have the same value.

The bits in $\{u_k\}_{k=1}^{P}$ and $\{u_k\}_{k=P+1}^{k=P+R}$ are encoded by constituent encoder A, while the bits in the $\{u_k\}_{k=P+1}^{k=P+R}$ and $\{u_k\}_{k=P+R+1}^{k=P+R+S}$ are encoded by constituent encoder B, and the bits in $\{u_k\}_{k=1}^{P}$ and $\{u_k\}_{k=P+R+1}^{k=P+R+S}$ are encoded by constituent encoder C. Moreover the information bits to constituent encoders B and C are interleaved before encoding. The constituent encoder is shown in figure 3.5.3.2.3.1-1.

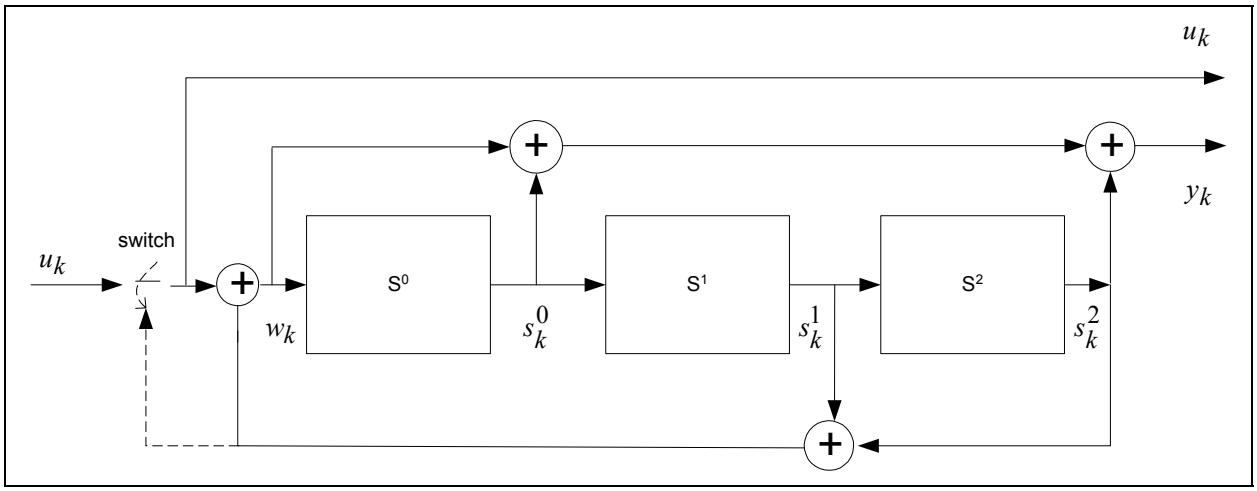


Figure 3.5. 3.2.3.1-1. Constituent Encoder (Dotted Lines Effective for Trellis Termination Only)

This is a Rate ½, systematic, recursive, convolutional code where the parity bit and next state equations are given by:

$$\begin{cases} y_k = w_k + s_k^0 + s_k^2 \\ s_{k+1}^2 = s_k^1, s_{k+1}^1 = s_k^0, \text{and } s_{k+1}^0 = w_k \\ w_k = u_k + s_k^1 + s_k^2 \end{cases}$$

3.5.3.2.3.2 Trellis Termination

Tail bits shall come from the current contents of the shift registers as shown in figure 3.5.3.2.3.1-1. Moreover, because of the Turbo interleaver, the contents of the shift that register at the beginning of trellis termination (after the encoding of information bits) are different for each constituent encoder. Therefore for the eight-state Turbo code (with three memory elements), a total of 3 x 3 = 9 tail input bits are required to terminate all three constituent encoders. Together with parity bits, a total of 9 x 2 = 18 bits are transmitted for trellis termination.

To represent the output of the Rate ½ turbo code the following notation is used:

Systematic bits before interleaving: u(1), u(2), u(3), …., u(L)
Transmitted parity bits of encoder A: $y_A(1)$, $y_A(3)$, $y_A(5)$, …, $y_A(2L/3-1)$
Transmitted parity bits of encoder B: $y_B(1)$, $y_B(3)$, $y_B(5)$, …, $y_B(2L/3-1)$
Transmitted parity bits of encoder C: $y_C(2)$, $y_C(4)$, $y_C(6)$, …, $y_C(2L/3)$
Systematic and parity tail bits of encoder A: $uT_A(0)$, $yT_A(0)$, $uT_A(1)$, $yT_A(1)$, $uT_A(2)$, $yT_A(2)$
Systematic and parity tail bits of encoder B: $uT_B(0)$, $yT_B(0)$, $uT_B(1)$, $yT_B(1)$, $uT_B(2)$, $yT_B(2)$
Systematic and parity tail bits of encoder C: $uT_C(0)$, $yT_C(0)$, $uT_C(1)$, $yT_C(1)$, $uT_C(2)$, $yT_C(2)$

The output bit representation for the Rate ½ turbo code is then:

:

u(1), y_A(1), u(2), y_A(3), ….,u(L/3), y_A(2L/3-1),
u(L/3+1), y_B(1), u(L/3+2), y_C(2), u(L/3+3), y_B(3),….,u(2L/3), y_C(L/3),
uT_A(0), yT_A(0), uT_A(1), yT_A(1), uT_A(2), yT_A(2),
u(2L/3+1), y_B(L/3+1), u(2L/3+2), y_C(L/3+2), u(2L/3+3), y_B(L/3+3),….,u(L),
y_C(2L/3),
uT_B(0), yT_B(0), uT_B(1), yT_B(1), uT_B(2), yT_B(2)
uT_C(0), yT_C(0), uT_C(1), yT_C(1), uT_C(2), yT_C(2)

3.5.3.2.3.3 Interleavers for Parser Output

The parser output sequence shall be interleaved before the encoder. The following steps describe the interleaver design where the input sequence in a burst can have an arbitrary length.

Step 1: Given a desired burst size of L, find the three integers P, R, and S, as follows:

$$\begin{cases} \text{if } (L \bmod 3) = 0, \text{ then, } P = R = S = L/3 \\ \text{if } (L \bmod 3) = 1, \text{ then, } P = (L-1)/3+1, R = S = (L-1)/3 \\ \text{if } (L \bmod 3) = 2, \text{ then, } P = R = (L-2)/3+1, S = (L-2)/3 \end{cases}$$

Step 2: Construct three interleavers - IP, IR, and IS - with sizes P, R, and S, respectively, and explained in the Note below.

Step 3: Interleaver B (denoted by IB) has size R+S and shall be formed by interlacing IR and an identity interleaver of size S. Interleaver C (denoted by IC) has size P+S and shall be formed by interlacing IP and IS.

The following shows an example where the interleaver is of size *L*=11.

Step 1: P = 4, R = 4, S = 3

Step 2: Suppose the interleaver tables IP, IR, and IS are constructed as follows:

IP = (1,3,0,2), IR = (2,0,3,1), IS = (2,0,1)

Step 3: IB = (2,4,0,5,3,6,1) and IC = (1,6,3,4,0,5,2)

Note: Procedure to obtain the interleaver tables *IP*, *IR,* and *IS*

First, determine two parameters, r and c, from table 3.5.3.2.3.3-1, which are a function of interleaver size *P* (R or S for *IR* and *IS* generation).

From r and c, create an integer i, which has $r+c$ bits that shall be:

$$i = \underbrace{b_0 b_1 b_2 \ldots b_{c-1} b_c \ldots b_{r+c-1}}_{r+c \quad bits}$$

Table 3.5.3.2.3.3-1 shows various interleaver sizes.

Table 3.5.3.2.3.3-1. Parameters R and C for Various Interleaver Size

Interleaver Size Interval	R	C
[64, 128]	4	3
[129, 208]	4	4
[209, 256]	5	3
[257, 416]	4	5
[417, 512]	5	4
[513, 1024]	5	5
[1025,2048]	5	6

Initially all bits are zero.

Take the first c bits in i and multiply by a constant v in table 3.5.3.2.3.3-2 determined by the bit-reversed last r bits of i. Then keep the last c (LSB) bits of the multiplication to get the last c bits of another $r+c$ bit integer variable j. The bit-reversed last r bits in i become the first r bits in j:

$$j = b_{r+c-1} b_{r+c-2} \ldots b_c \tilde{b}_0 \tilde{b}_1 \ldots \tilde{b}_{c-1} \quad \text{where} \quad \tilde{b}_0 \tilde{b}_1 \ldots \tilde{b}_{c-1} = LSB[k * (b_0 b_1 \ldots b_{c-1})]$$

If j is less than P, accept it to the interleaver table as (i, j); otherwise, discard it.

Increment the i by 1 ($i = i + 1$) and repeat steps 3 and 4 until all P values of the interleaver table are obtained.

Table 3.5.3.2.3.3-2 shows values for various interleaver sizes.

Table 3.5.3.2.3.3-2. Values for Various Interleaver Sizes

[64-128]			[129-208]			[209-256]			[257-416]			[417-512]			[513-1024]			[1025-2048]		
P	R	S	P	R	S	P	R	S	P	R	S	P	R	S	P	R	S	P	R	S
1	5	7	5	9	13	1	5	7	11	25	13	9	5	11	29	1	27	55	57	9
3	3	5	13	1	3	3	3	5	21	17	1	3	11	7	1	13	15	13	1	43
5	7	1	7	5	15	5	7	1	7	9	3	13	1	1	27	17	19	7	15	35
7	1	3	1	11	7	7	1	3	29	3	19	7	7	9	5	9	3	59	23	23
5	7	1	11	13	5	5	7	1	1	15	29	11	3	3	11	19	5	15	49	7
7	1	3	15	3	1	7	1	3	15	11	17	1	5	7	17	27	9	11	33	21
1	5	7	3	7	11	1	5	7	17	23	7	3	9	5	3	5	13	61	61	53
3	3	5	9	15	9	3	3	5	13	31	21	15	13	13	7	29	17	27	3	19
3	1	5	11	7	11	3	1	5	27	19	31	9	15	11	21	21	5	35	11	61
5	5	1	3	11	5	5	5	1	5	1	5	1	7	3	19	31	31	31	19	25
7	3	3	7	1	9	7	3	3	3	27	25	7	1	1	13	5	25	51	29	1
1	7	7	13	9	13	1	7	7	23	13	23	13	9	5	1	13	15	3	41	11
7	3	3	5	15	7	7	3	3	9	5	9	7	13	7	7	11	13	17	63	29
1	7	7	9	13	1	1	7	7	19	21	15	5	15	13	23	25	11	39	7	39
3	1	5	15	3	15	3	1	5	25	7	27	11	3	9	15	7	9	49	31	41
5	5	1	1	5	3	5	5	1	31	29	11	9	1	3	9	23	1	41	35	59
						3	1	7				15	7	15	29	3	27	21	55	63
						1	1	5				3	3	11	31	15	19	63	25	17
						3	7	3				3	9	1	3	19	29	9	45	27
						5	3	1				7	5	13	13	25	23	1	21	45
						7	5	1				11	13	5	19	31	11	19	17	51
						1	1	3				1	11	11	27	29	7	33	39	13

[64-128]			[129-208]			[209-256]			[257-416]			[417-512]			[513-1024]			[1025-2048]		
P	R	S	P	R	S	P	R	S	P	R	S	P	R	S	P	R	S	P	R	S
						1	7	7				5	15	13	17	1	25	47	51	57
						5	3	7				15	3	9	5	23	21	23	5	3
						5	7	5				15	1	15	11	3	17	29	27	49
						1	5	1				11	15	7	23	9	23	5	37	31
						7	5	5				1	9	3	31	11	1	57	13	15
						7	1	3				5	5	9	25	15	31	43	9	5
						3	3	7				9	7	1	9	17	3	25	59	33
						5	3	3				13	11	5	25	21	7	53	53	55
						7	5	5				5	13	15	15	27	29	37	47	47
						3	7	1				13	11	15	21	7	21	45	43	37

3.5.3.2.3.4 Puncturing

The output bits of each constituent encoder are punctured to achieve the desired code rate. For IPoS, code Rate ½ shall be achieved by transmitting all information bits $\{u_k\}_{k=1}^{k=L}$, while every other bit of encoder output shall be punctured. (A puncturing pattern of 10 is applied to the first two encoder outputs, whereas a pattern of 01 shall be applied to the last encoder outputs.) This gives a code Rate $1/\{1+2/3\cdot 1/2+2/3\cdot 1/2+2/3\cdot 1/2\}=1/2$.

3.5.3.2.4 Channel Interleaver

The channel interleaver is a block interleaver and shall have a size as large as 2048 bits. The channel interleaver shall interleave on the bit, not the symbol, boundary. Where the burst (or subburst) size of the encoded bits is greater than 2048 bits, the burst size shall be partitioned into two equal segments. If the segments are still greater than 2048 bits in size, then each segment is further divided into two equal parts. For various encoded burst sizes of E bits, the encoded bit sequence shall be segmented into the following lengths to remain within the maximum interleaver size limit:

E	for 0 bit < $E \le 2048$ bits
$E/2$, $E/2$	for 2048 bits < $E \le 4096$ bits
$E/4+1$, $E/4+1$, $E/4$, $E/4$	for 4096 bits < $E \le 8192$ bits
$E/8+1$, $E/8+1$, $E/8$, $E/8$, $E/8$, $E/8$, $E/8$, $E/8$	for 8192 bits < $E \le 12306$ bits

For each data segment, the actual interleaver size shall be the smallest power of 2 greater than the segment size. When possible, the number of columns shall be the same as the number of rows. When it is not possible, the number of columns shall be twice as many as the number of rows. Table 3.5.3.2.4-1 illustrates the size of the interleaver.

Table 3.5.3.2.4-1. Channel Interleaver Sizes (Example)

Size (Number of Encoded Bits)	Number Rows	Number Columns
Less than 257	16	16
257 to 512	16	32
513 to 1024	32	32
1025 to 2048	32	64

The data shall be written into the interleaver from the lowest numbered column to the highest numbered column of the lowest numbered row before proceeding to filling the next higher numbered row. The interleaved data are read from the interleaver from the lowest numbered row to the highest numbered row of the lowest numbered column before proceeding to output the next higher numbered column. If a location of the interleaver has not been written to, that location shall be skipped during the interleaved output sequence.

3.5.4 Inroute Framing Structure

In the inroute link, IPoS uses a periodic TDMA structure that permits several remotes to share the same inroute carrier or group of inroute carriers. This TDMA structure includes:

- A frame duration of 45 msec
- A superframe consisting of eight frames with a duration of 8 * 45 = 360 msec

Each frame is divided into slots. The number of slots per frame, N, depends upon the transmission rate and the type of encoding used in the payload of the burst. Figure 3.5.4-1 illustrates inroute framing.

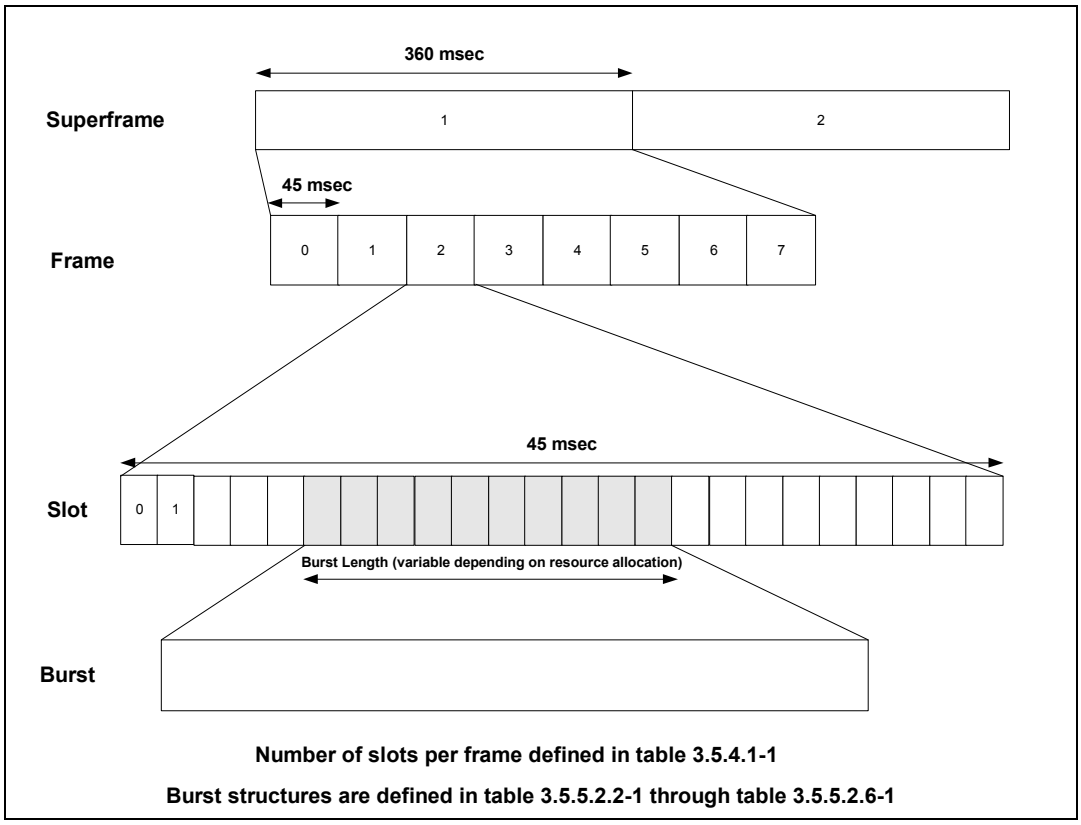


Figure 3.5.4-1. Turbo Code Inroute Framing Structure

3.5.4.1 TDMA Slots

Table 3.5.4.1-1 shows the number of slots per frame, the duration of the slots, and the number of modulated symbols for the different transmission rate and coding schemes.

Table 3.5.4.1-1. IPoS Inroutes TDMA Characteristics

FEC Encoding	Symbol Rate	Slots/Frame	User Bytes/Slot	Bits/Slot	Symbols/Slot	Slot Time
½ Con.	64 ksps	51	7	112	56	875 μs
½ Con.	128 ksps	90	8	128	64	500 μs
½ Con.	256 ksps	160	9	144	72	281.25 μs
½ Turbo	128 ksps	80	9	144	72	562.5 μs
½ Turbo	256 ksps	160	9	144	72	281.25 μs

The slot designator number starts at 0 and ends at N1.

3.5.5 Burst Formats

Two types of burst are used in the inroute direction:

1. The user burst is used for data traffic over the inroute channels.

2. Ranging burst used by remotes to obtain delay and power information and to carry resource requests to the IPoS hub.

Each of these types of burst is associated with a different time uncertainty in its arrival at the hub or aperture, but each one uses the same burst format with different data in the payload. This time uncertainty associated with the misalignment of the timing between the hub and remotes and the uncertainties in the satellite position are designated as aperture. The distinction between Ranging and User bursts is defined by the Burst Allocation Packet (BAP) defined in Section 4 of this standard.

3.5.5.1 Apertures

The imprecision in the arrival of the inroute bursts at the hub defined at the slot boundaries is designated as the aperture. Two apertures are defined:

1. The user data burst aperture of 125 microseconds
2. The ranging burst aperture of 2 milliseconds

3.5.5.2 User Data Burst Structure

Inroute transmissions are made with variable-length bursts occupying one or more consecutive slots in the frame using either convolutional or Turbo coding.

The elements in the burst for convolutional-coded bursts are illustrated by figure 3.5.5.2-1 and figure 3.5.5.2-2.

Figure 3.5.5.2-1 illustrates the burst format for inroute convolutionally coded bursts at the transmission rate of 64 ksps.

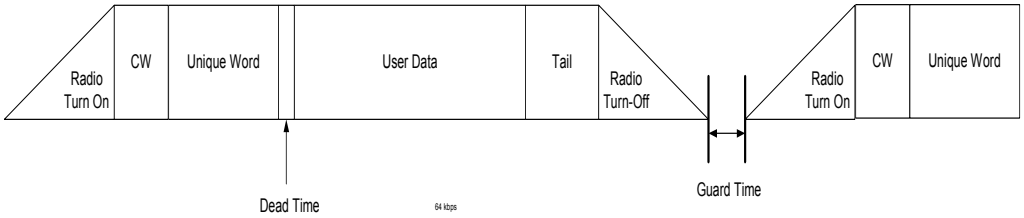


Figure 3.5.5.2-1. 64 ksps Convolutionally Coded Burst Elements

Figure 3.5.5.2-2 illustrates the burst format for the inroute convolutionally and Turbo-coded burst at the transmission rate of 128 and 256 ksps.

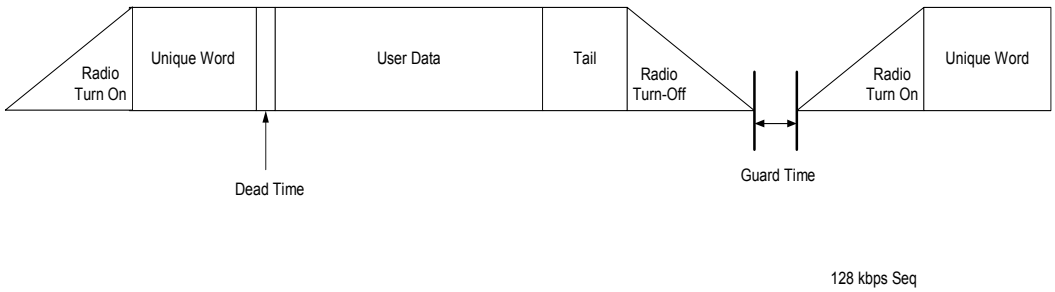


Figure 3.5.5.2-2. 128 ksps and 256 ksps Convolutionally and Turbo-Coded Burst Elements

The burst formats for both convolutionally and Turbo-coded IPoS inroutes include the following elements:

- Guard time or minimum separation between consecutive bursts.
- Radio turn-on or ramp-up time to control the emission of the burst.
- Radio turn-off or ramp-down period to control the emissions of the burst.
- The 64 ksps convolutional-coded burst starts with a continuous wave (CW).
- The UW is the preamble used to perform PHY processes related to frequency estimation, time estimation, and the estimation of the beginning of the burst.
- Payload is used to convey encoded information for the higher layers.
- Tail bits used to flush the encoders.

The duration of a burst payload is an integer number of slots from 1-to-N1 slots in the frame.

3.5.5.2.1 Burst Time Alignment

The inroute bursts are transmitted by the IPoS remote with their payloads aligned to the boundaries of the slots of the frame as shown in figure 3.5.5.2.1-1.

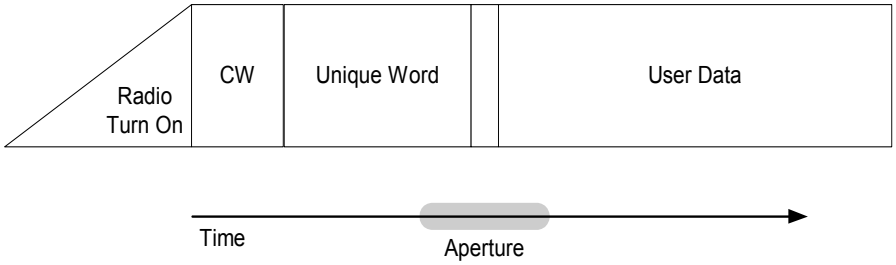


Figure 3.5.5.2.1-1. IPoS Slot Frame Boundaries

The burst transmitted by a remote terminal begins at the end of the first slot allocated to the terminal for inroute transmission; the payload begins at the beginning of the second allocated slot and extends to the last allocated slot. The tail and the turnoff time of the burst are sent in a slot that is not allocated to the terminal but that is unused by the beginning of the burst from the next-allocated terminal.

At the IPoS hub, the maximum misalignment between the received burst and the frame boundaries is the aperture of the corresponding burst. Figure 3.5.5.2.1-2 illustrates this misalignment between bursts.

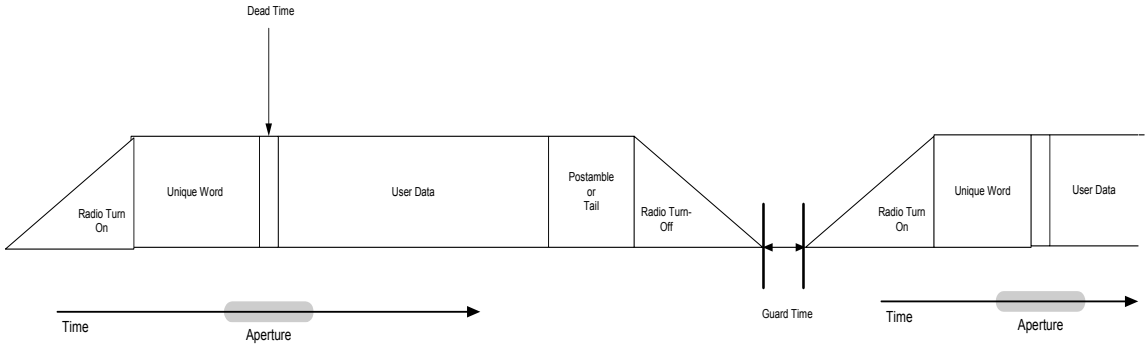


Figure 3.5.5.2.1-2. Multiple Bursts Received Time Misalignment at IPoS Hub, 128 ksps and 256 ksps

3.5.5.2.2 Burst Structure for 64 ksps Convolutional Coding

The frame overhead is sized as two slots (112 bits) minus the aperture size. The aperture size is 8 bits. See table 3.5.5.2.2-1.

Table 3.5.5.2.2-1. Burst Structure for 64 ksps

Field	Symbols	Microseconds	Comments
Radio Turn-on	2	31.3	
Continuous Wave	55	859.4	
Unique Word	24	375.0	Unique word needed for burst acquisition
Dead Time	3	46.9	All 1s
Payload	56*N	875*N	Each slot is 7 bytes of user traffic
Postamble (or Tail)	18	281.3	Parity bits at the end of the burst
Radio Turn-off	2	31.3	

3.5.5.2.3 128 ksps Service Burst Structure – Convolutional

The frame overhead is sized as one slot (64 bits) minus the aperture size. The aperture size is 16 bits. See table 3.5.5.2.3-1.

Table 3.5.5.2.3-1. Burst Structure 128 ksps - Convolutional

Field	Symbols	Microseconds	Comments
Radio Turn-on	3	23.4	
Unique Word	24	187.5	Unique word needed for burst acquisition

Table 3.5.5.2.3-1. Burst Structure 128 ksps - Convolutional

Field	Symbols	Microseconds	Comments
Dead Time	3	23.4	All 1s
Payload	64*N	500*N	Each slot is 8 bytes of user traffic
Postamble (or Tail)	18	140.6	Parity bits at the end of the burst
Radio Turn-off	3	23.4	

3.5.5.2.4 128 ksps Service Burst Structure – Turbo

The frame overhead is one slot, with 80 slots per 45-millisecond frame. The Tail and radio Turn-off are sent in a slot not allocated to the site, but this is allowed since the first portion of the next-allocated slot is unused because it is the beginning of a burst. See table 3.5.5.2.4-1.

Table 3.5.5.2.4-1. Burst Structure for 128 ksps - Turbo

Field	Symbols	Microseconds	Comments
Radio on	3	23.4	
Unique Word	24	187.5	Unique word needed for burst acquisition
Dead Time	0		
Turbo-Coded Payload	72*N	562.5*N	Each slot is 9 bytes of user traffic
Postamble (or Tail)	9	70.3	
Radio Turn-off	3.2	25	

3.5.5.2.5 256 ksps Service Burst Structure – Convolutional

The frame overhead is sized as one slot (72 bits) minus the aperture size and radio Turn-on and Turn-off guard time. The aperture size is 32 bits. See table 3.5.5.2.5-1.

Table 3.5.5.2.5-1. Burst Structure for 256 ksps Convolutional

Field	Symbols	Microseconds	Comments
Radio Turn-on	6.5	25.4	
Unique Word	16	62.5	UW needed for burst acquisition
Dead Time	3	11.7	All 1s
Payload	72*N	281.25*N	Each slot is 9 bytes of user traffic
Postamble (or Tail)	18	70.3	Parity bits at the end of the burst
Radio Turn-off	6.5	25.4	

3.5.5.2.6 256 ksps Service Burst Structure – Turbo

The frame overhead is one slot, with 160 slots per 45-millisecond frame. However, a burst cannot continue through the middle of the frame time. Therefore, the 81st slot must either be the beginning of a burst or left unused. The Tail and radio Turn-off are sent in a slot not allocated to the site, but this is allowed since the first portion of the next allocated slot is unused since it is the beginning of a burst. See table 3.5.5.2.6-1.

Table 3.5.5.2.6-1 Burst Structure for 256 ksps Turbo

Field	Symbols	Microseconds	Comments
Radio on	5.9	23.0	
Unique Word	24	93.8	Unique word needed for burst acquisition
Dead Time	0		
Turbo-Coded Payload	72*N	281.25*N	Each slot is 9 bytes of user traffic
Postamble (or Tail)	9	35.2	
Radio Turn-off	6.4	25	

3.6 Physical Layer Measurements

The PHY parameter included in this subsection shall be monitored in the PHY and reported to a higher layer for support in the higher-layer procedures.

3.6.1 Outroute Bit Error Rate

The remote shall measure the received $\frac{E_{bt}}{N_0}$ of the outroute carrier to an accuracy of ± 0.2 dB.

3.6.2 Signal Quality Factor

The Signal Quality Factor (SQF) provides the IPoS terminal's installer and user with an easy-to-understand estimation of the quality of the received outroute signal. To maintain consistency among the various IPoS remote brands and their signal strength readings, the IPoS remote shall display the relationship of E_{bt}/N_o to SQF as defined by table 3.6.2-1 and figure 3.6.2-1.

Table 3.6.2-1. Required Relationship Between E_{bt}/N_o (dB) and SQF

E_{bt}/N_o	SQF
0.5	31
1	33
1.5	35
2	38
2.5	41
3	45
3.5	49
4	53
4.5	57
5	61
5.5	65
6	69
6.5	73
7	77
7.5	80

Table 3.6.2-1. Required Relationship Between E_{bt}/N_o (dB) and SQF

E_{bt}/N_o	SQF
8	84
8.5	87
9	89
9.5	92
10	94
10.5	95
11	97
11.5	98
12	98
12.5	99
13	99
13.5	99
14	99

Figure 3.6.2-1 illustrates the relationship between E_{bt}/N_o and SQF.

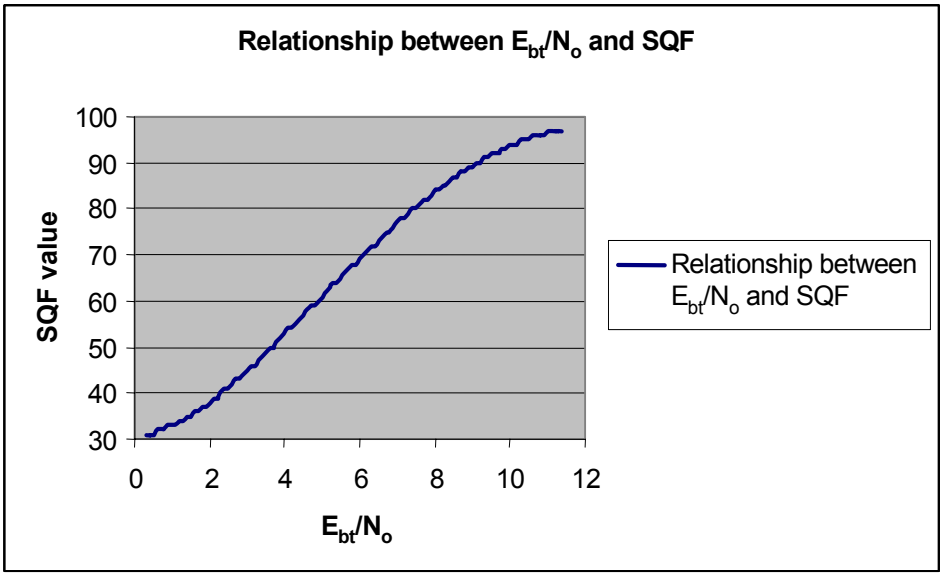


Figure 3.6.2-1. Required Relationship Between E_{bt}/N_o and SQF

3.7 Interface to Higher Layers

The following subsections describe the specific primitives used by the PHY to exchange information with the higher layers of the IPoS protocol stack.

3.7.1 User Plane Primitives

The PHY uses the following primitives across the interface with the MAC sublayer over the user plane:

PHY-U-DATA-REQ

Used to pass information flows between physical and MAC layers.

PHY-U-DATA-IND

Indicates that the data transfer has been completed.

3.7.2 Control Plane Primitives

The PHY uses the following primitives across the interface with the MAC sublayer over the control plane:

PHY-C-Inroute Radio Power Control-REQ

The IPoS remote shall have output power control. This power control shall allow control via messaging sent on the outroute.

PHY-C-Inroute Radio Power Control-RES

Upon command, the IPoS remote shall be able to measure its output power to within 0.2 dB of the commanded value.

PHY-C-Inroute Radio Power Control-IND

The IPoS remote shall indicate that it has implemented the power control command.

PHY-C-Outroute FEC Control-RES

The IPoS remote shall set itself automatically to the correct FEC rate for the outroute.

PHY-C-Outroute FEC Control-IND

The IPoS remote shall provide current outroute FEC rate information to higher levels of the IPoS protocol stack.

PHY-C-Outroute FEC Change-RES

Upon sensing a change in the FEC rate, the IPoS remote shall change automatically to that rate and demodulate data.

PHY-C-Outroute Symbol Rate-RES

The transmit symbol rate of the outroute shall be able to be set by DLL protocols.

PHY-C-Outroute Symbol Clock-IND

The IPoS remote shall indicate that it has recovered the symbol clock to act as a source of clocking information and the symbol rate being demodulated.

PHY-C-Outroute Frequency Lock Loop-IND

The IPoS remote indicates the status of the demodulator's FLL. The status types shall be locked and unlocked.

PHY-C-Outroute Demodulator Unlock-IND

The IPoS remote indicates the status of the demodulator. The status types shall be locked and unlocked.

PHY-C-Inroute Burst Time Management-REQ

The IPoS remote shall be able to control the timing of each data burst under control from the data sent on the outroute. This data and the required timing for this data are specified in the inroute data link layer definition.

PHY-C-Inroute Burst Time Management-IND

The IPoS remote PHY shall indicate that it has used the data burst timing required by higher levels of the IPoS protocol stack.

PHY-C-Inroute Burst Frequency Management-RES

The IPoS remote shall be able to control the frequency of each data burst under control from the outroute data. This data and the required frequency for this data are specified in the inroute data link layer definition.

PHY-C-Inroute Burst Frequency Management-IND

The IPoS remote shall indicate the burst frequency used for each burst.

3.7.3 Management Plane Primitives

The physical layer uses the following primitives across the interface with the management entity:

PHY-M-Activate Outroute-REQ

For the activation of the activation of the outroute acquisition.

PHY-M-Activate Outroute-IND

Indication that the outroute is activated.

PHY-M-Activate Inroute-REQ

For the activation of the inroute transmissions.

PHY-M-Activate Inroute-IND

Indication that inroute transmissions are activated.

PHY-M-Deactivate Outroute-REQ

Deactivate the outroute reception.

PHY-M-Deactivate Outroute-IND

Indication that the outroute reception is deactivated.

PHY-M-Deactivate Inroute-REQ

Deactivate the inroute transmissions.

PHY-M-Deactivate Inroute-IND

Indication that the inroute transmitter is deactivated.

PHY-M-Inroute Transmitter Frame Count-REQ

The IPoS remote shall record the transmitted frame count.

PHY-M-Inroute Transmitter Frame Count-IND

The IPoS remote shall indicate the frame count that was transmitted.

PHY-M-Inroute Transmitter Reset-REQ

The IPoS remote shall reset its transmitter.

PHY-M-Inroute Transmitter Reset-IND

The IPoS remote shall indicate that its transmitter has been reset.

PHY-M-Inroute Transmitter Reset Count-IND

The IPoS remote shall record the number of times the transmitter was reset.

3.8 Physical Layer Procedures

3.8.1 Timing Synchronization

Timing synchronization is used to align the transmission of the remote terminals with the superframe, frame, and slot structure of the inroute carriers. This alignment is composed of the following procedures:

- Outroute carrier acquisition
- Inroute frame alignment
- Ranging

3.8.1.1 Outroute Carrier Acquisition

During the commissioning procedure, the remote terminal is provided with parameters that allow the acquisition and demodulation of the information conveyed by outroute carrier. These parameters include:

- Frequency, polarization, and symbol rate of the outroute carrier: Used for the tuning and acquisition of the outroute carrier.
- The program identifiers: Used by the remote to prefilter the control and traffic information contained in the outroute.
- Hub IP address: Used to transmit data to the proper hub.
- IP addresses assigned to the terminal: Used by the hub to process data for this terminal.

After commissioning, the reception of the outroute carrier shall be activated to permit its acquisition. This outroute carrier acquisition provides the remote terminal with:

- The symbol clock of the demodulated carrier to be used for the frequency stability of the local frequency reference used to derive the frequency of the inroute carriers
- The information in the channels with the PID addresses monitored for the terminal
- Reception of the superframe numbering packets transmitted by the hub every 360 msec at the beginning of every superframe
- Verification that the received outroute matches the commissioning parameters

3.8.1.2 Inroute Frame Alignment

Frame timing synchronization is the process of aligning the IPoS remote terminal transmissions with an internal timing reference that is used at the IPoS hub to generate the outroute superframe and the inroute framing used by the hub demodulator equipment.

Subsection 4.12.1 describes the system timing procedures performed by remote terminals to determine when they should transmit so that their transmissions arrive aligned with the reference framing established by the hub for each of the groups of inroute carriers used by remote terminals in the inroute direction.

3.8.1.3 Inroute Burst Synchronization

Ranging is used to fine-tune an IPoS remote's transmission timing in order that the remote terminal transmissions are received at the proper instant at the hub.

The ranging procedures are described in Subsection 4.12.2. They provide the remote terminals with the timing correction and the power level they need to use for inroute transmissions.

Ranging procedures shall be triggered upon the following events:

- The first time the remote terminals operate from a particular location
- When the remote terminal uses a different satellite
- When the hub remote terminal detects error conditions where propagation delay may be a factor.

4 DATA LINK LAYER

4.1 Scope

The present document is the detailed specification of the MAC/SLC layer protocol for the IPoS air interface. In particular, it contains MAC and SLC procedures, messages, and message formats.

4.2 Data Link Control Overview

The DLC provides the higher protocol layers with IP transfer capabilities for signaling and user data over the logical channels defined in the IPoS air interface. The DLC layer is further subdivided into the following sublayers:

- MAC sublayer that provides the format and data structure used to encapsulate the user and control the information over the packets and bursts defined over the PHY. This layer includes a multiplexing sublayer that is defined only in the outroute direction

- SLC sublayer that provides the communication protocols used to provide reliable transfers and the shared access of channels among multiple IPoS terminals.

The general architecture of the DLC and its relationship with other layers is shown from the IPoS terminal perspective in figure 4.2-1.

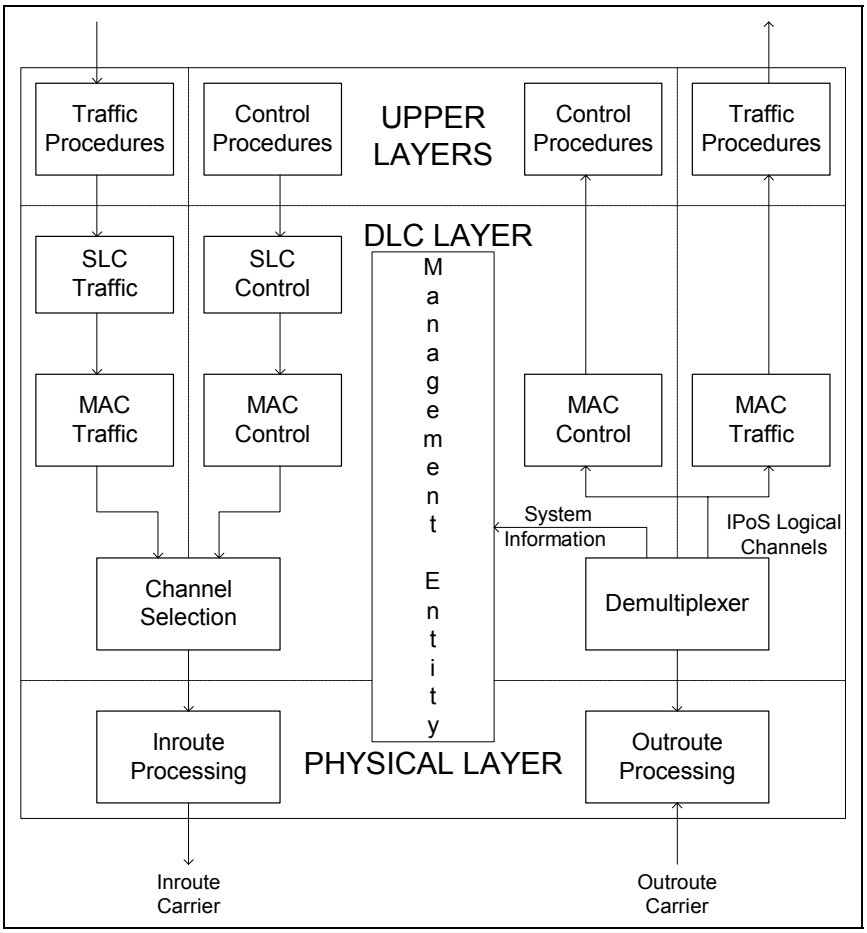


Figure 4.2-1. DLC Model

The DLC is modeled from an IPoS terminal view in three planes (user, control, and management) for both transmission directions:

- Outroute: The hub transmissions are received by all IPoS terminals.
- Inroute: The hub receives transmissions from IPoS terminals.

4.3 Satellite Link Control Sublayer

4.3.1 Overview

The SLC layer is the sublayer of the DLC layer that is responsible for end-to-end transmission and reception of IP packets between IPoS remote terminals and the hub. It supports reliable delivery in the remote-to-hub direction and unreliable delivery in the hub-to-remote direction.

4.4 Modes of Operation

4.4.1 Registration and Commissioning

Registration and commissioning for IPoS remote terminals are accomplished by following these steps:

1. Configuring the unique data for this terminal at the hub and at the terminal, as subsection 4.14 describes. This includes the remote terminal's encrypted key at the hub.
2. The hub transmits the encrypted keys periodically for all remote terminals on the outroute periodically. The keys are encrypted with the remote terminal's hard-coded secret data so that only the specified terminal can decrypt the key.
3. The remote terminal is installed at the remote location.
4. The remote terminal receives the encrypted keys (unicast and multicast) that are specified on the outroute for its serial number. IPoS serial numbers are unique across an IPoS system.
5. The remote terminal stores the encrypted keys in nonvolatile memory.
6. The remote terminal installs its encrypted keys in its decryption hardware. The decryption hardware decrypts the key and installs it in the decryption hardware so that it can begin decrypting the outroute data.

At this point, the IPoS terminal is ready to begin operation in the IPoS system. Note that there is no terminal authentication procedure required. An unauthorized terminal will not have the secret key data that the authorized terminal has, so it will not be able to decode outroute data.

4.4.2 IPoS Terminal Startup

To begin operation in an IPoS system, an IPoS terminal follows these steps:

1. Acquires timing and frequency with the outroute configured for it.
2. Installs the encrypted keys from nonvolatile memory so that it will be able to decrypt outroute data.
3. Receives system information including frame timing, inroute frequency, timing, and modulation timing.
4. Installs the proper DVB MAC filter addresses in its receiver so that it will receive only information that may be relevant to this particular terminal.

5. Performs a ranging procedure with the hub to determine its transmit timing parameters so that it can transmit inroute bursts that will be synchronized with the hub's frame timing. Note that the IPoS terminal does not use the satellite ephemeris.

4.4.3 IP Packet Delivery

Once a remote terminal has followed the startup procedure, its SLC layer is ready to accept IP packets for delivery to the hub at its upper-layer SAP. Similarly, the hub's SLC layer is ready to accept IP packets for delivery to remote terminal(s) at its upper layer SAP. The hub and remote terminals are also ready to receive IP packets from the SLC's upper layer SAP. Note that there is no concept of access session over the air interface, meaning that IP connectivity between the remote terminals to the IP backbone is always on after the startup procedures are completed. Remote terminals exchange control packets with the hub to establish a communication session when they need bandwidth assigned to send IP data packets. That is, there is no sign-on or authentication each time the hub and remote terminal need to exchange IP packets.

4.5 Compression

The IPoS system can be used optionally with data or IP header compression. Data compression would take place above the SLC layer, so it is outside the scope of this document. IP header compression is also outside the scope of this document.

4.6 Interface with Higher Layers: SI-SAP

4.6.1 Overview

The IP layer, which is directly above the DLC layer, uses this SAP to communicate with the DLC. This SAP is a subset of the SI-SAP that reference [2] (found in subsection 1.4 of this document) describes. The IPoS uses this standard SAP so that software or devices that use this SAP can be modified more easily to use another satellite system that implements the same standard SAP.

The SI-SAP contains a number of features that do not apply to the IPoS system architecture or are not implemented in the IPoS system. The following subsections describe the specific SI-SAP primitives that the IPoS system uses.

4.6.2 User Plane

The IPoS system uses the following U-Plane primitives:

- **SI-U-DATA-REQ**: The IP layer, at both the hub and remote terminals, uses this primitive to send an IP packet to the DLC. The parameters are used as follows:
  - Destination MAC address: Used only at the hub to specify the particular IPoS terminal (for unicast) or terminals (for multicast) that should receive and process the data.
  - CoS Tags: Not currently used
  - Connection ID: Not currently used
  - SDU: IP packet for transmission
- **SI-U-DATA-IND**: The IP layer, at both the hub and remote terminals, uses this primitive to receive an IP packet from the DLC. The parameters used are as follows:
  - Destination MAC Address: Address as specified at the hub (remote terminal only)
  - CoS Tags: Not currently used
  - Connection ID: Not currently used
  - SDU: IP packet being received

4.6.3 Control Plane

4.6.3.1 Flow Control

The IPoS system uses the following flow control primitives:

- **SI-C-CREDIT**: The IP layer at the hub and remote terminals uses this primitive to request credits to send IP packets to the DLC layer. The parameters are used as follows:
  - Credit Request ID
  - Flow Control ID
  - Destination Address: Not currently used
  - CoS Tags: Not currently used
  - Credit
  - Credit Expiry Timer

- **SI-C-CREDIT_RESET**: The DLC layer can cancel an existing credit using this primitive. The parameters are used as follows:
  - Flow Control ID

4.6.3.2 Multicast Control

The IPoS system uses the following Multicast Control primitives:

- **SI-C-JOIN**: The IP layer at the remote terminals only uses this primitive to request joining a multicast that the hub is transmitting. The parameters are used as follows:
  - Multicast Network Address: IP multicast destination address
  - User-to-User Signaling: Not currently used
- **SI-C-JOIN_ACCEPT**: The DLC layer at the remote terminals only uses this primitive to accept an SI-C-JOIN request. The parameters are used as follows:
  - Multicast Network Address: IP multicast destination address
  - Multicast Port ID: Not currently used
- **SI-C-JOIN_REJECT**: The DLC layer at the remote terminals only uses this primitive to reject an SI-C-JOIN request. The parameters are used as follows:
  - Multicast Network Address: IP multicast destination address
  - Cause Code
- **SI-C-PRUNE**: The IP layer at the remote terminals only uses this primitive to request to leave a multicast that it previously joined. The parameters are used as follows:
  - Multicast Network Address: IP multicast destination address
  - User-to-User signaling: Not currently used
- **SI-C-PRUNE_ACCEPT**: The DLC layer at the remote terminals only uses this primitive to accept an SI-C-PRUNE request; the parameters are used as follows:
  - Multicast Network Address: IP multicast destination address
  - Multicast Port ID: Not currently used

- **SI-C-PRUNE _REJECT**: The DLC layer at the remote terminals only uses this primitive to reject an SI-C-PRUNE request. The parameters are used as follows:
  - Multicast Network Address: IP multicast destination address
  - Cause Code

4.6.3.3 Management Plane

The IPoS system uses the following Management Plane primitives:

- **SI-M-REMOTE**: This is a generic management primitive used as a place holder. The parameters are used as follows:
  - Sequence Number
  - IP Packet

4.7 Media Access Control Sublayer

4.7.1 Overview

MAC is a sublayer of the DLC layer. This layer shall control the way an IPoS terminal uses its inroute resources, i.e., Aloha contention channel, and processes the DVB outroute. This layer handles the following functions:

- Outroute
  - IPoS DVB PID information
  - IP packet segmentation and reassembly
  - Data encryption and decryption
  - Discriminate and filter traffic received by the IPoS terminal
  - Multiplex and demultiplex logical control channels
- Inroute
  - Request and allocate bandwidth
  - Transmit and receive data bursts
  - IP packet segmentation and reassembly

4.8 Interfaces, SAPs, Service Definitions, and Service Primitives

This subsection gives details of different interfaces that the MAC sublayer has with other layers and entities.

4.8.1 MAC Interface with Physical Layer

4.8.1.1 Service Access Point

The IPoS reference model defines a SAP between the MAC and the PHY. This SAP shall provide the means for transfer of IP packets, control, and management information between the MAC and the PHY for transmission over the air link.

4.8.1.2 Services

The MAC sublayer expects the following services from the PHY:

- Transmission/reception of MAC PDUs on the assigned logical channel
- Current status of radio link

4.8.1.3 Primitives

The primitives between the MAC and the PHY are given in subsection 3.7.

4.8.2 Interfaces with Layer Management Entities

The MAC sublayer uses the following primitives across the interface with the management entity:

MAC-M-DATA-REQ

Used to transfer system information between the MAC and the management plane.

MAC-M-DATA-IND

Indicates that the transfer has been completed.

MAC-M-ERROR-IND

This primitive provides error reports on events such as retransmissions, discarded PDUs, etc.

MAC-M-ESTABLISH-REQ

Used by the management entity to request the establishment of individual logical channels.

MAC-M-ESTABLISH-IND

Indicates that the individual logical channels have been established.

MAC-M-RELEASE-REQ

Used by the management entity to request the release of individual logical channels.

MAC-M-RELEASE-IND

Indicates the release of logical channels.

MAC-M- ADJUST-REQ

Used by the management entity to set the operational parameters of the logical channels.

4.8.3 Logical Interfaces with Peer Layer

The peer-to-MAC sublayer of an ST resides in the network. The ST interacts with the bandwidth control component on the satellite over the U-Interface for negotiating the required channel and bandwidth for both the rate and volume traffic.

This logical interface shall be supported with the set of messages listed in subsections 4.11 and 4.13.

4.9 Outroute Multiplexing

Multiple programs, services, or types of information are multiplexed within the same outroute carrier. The outroute multiplexer sublayer statistically multiplexes information streams specific to the IPoS system with other MPEG-encoded video or data streams.

The higher layer information in these programs is mapped by the multiplexing sublayer into a continuous transport stream of packets that interfaces with the PHY. This transport stream consists of DVB/MPEG compliant packets (see reference [1], found in subsection 1.4 of this document) with the following characteristics:

- Fixed-length packets of 188 bytes containing a 4-byte DVB/MPEG header and 184 bytes available for payload.
- Fixed symbol transmission rate as determined by the PHY.

- Individual program information mapped to an integer number of packets; no packet contains information from two different programs.

- Packets from different programs and services are statistically multiplexed in the outroute transmission stream; there is no fixed allocation or relationship between a program and the position of its packets in the transport stream.

- Always-on outroute, null-packets are inserted in the transport stream when there is no information from the programs.

Outroute DVB/MPEG packets are broadcast over the entire outroute carrier bandwidth with IPoS terminals filtering those packets that do not match their own addresses. The addressing scheme is included as part of the transport packet header and MAC header.

4.9.1 Transport Packet Header

The 4-byte header of the DVB/MPEG transport packet is transmitted at the beginning of the 188-byte packet. The fields and values used in IPoS for the DVB/MPEG transport packet header are compliant with reference [1] (found in subsection 1.4 of this document), and defined in table 4.9.1-1.

Table 4.9.1-1. DVB/MPEG Transport Packet Header

Field Name	Field Length (bits)
synch_byte	8
transport_error_indicator	1
payload_unit_start_indicator	1
transport_priority	1
PID	13
transport_scrambling_control	2
adaptation_field_control	2
continuity_counter	4

The description of the fields in the transport packet header is as follows:

- synch_byte: Set to 0x47. This fixed 8-bit field is defined by the PHY.

- transport_error_indicator: Set to '0'. When set to '1' this 1-bit flag indicates that the packet contains an uncorrectable error.

- payload_unit_start_indicator: Set to '1'. If the payload includes IPoS-specific information, the bit indicates that the payload starts immediately after the packet header. If the packet contains a Program Specific Information (PSI) table, this bit indicates that the first byte of the payload carries a pointer with the number of bytes to the beginning of the section.

- PID: The value of this 13-bit field contains the PID, as defined in the next subsection.

- transport_scrambling_control: In the case of a null packet, this field is set to '00'; all other combinations indicate "user-defined." Any of the "user defined" values might be used in IPoS.

- adaptation_field_control: Set to '01', "payload only," for IPoS-specific PIDs, and '11' "adaptation field followed by payload" for PSI tables.

- continuity_counter: Set to '0000' for IPoS specific payloads. For PSI tables, this 4-bit field increments wrapping around to zero after taking the maximum value.

4.9.2 Program Identifiers

The 4-byte DVB/MPEG header includes a 13-bit PID field intended to support the multiplexing of diverse programs or services such as video or data programs over the same outroute carrier. The PID field in the packet header identifies the program, which permits the terminals associated with a particular outroute carrier to receive one or more programs by filtering packets based on the PID field.

IPoS outroute carriers multiplex two types of relevant information to the IPoS terminals:

- PSI tables, which provide both IPoS and non-IPoS terminals with configuration of services. The IPoS terminals receive the PSI tables to determine the specific configuration of the IPoS system.

- IPoS user and control information, which is transported in the IPoS logical channels. The information contained in the IPoS logical channels can be targeted to all, a group, or individual IPoS terminals.

IPoS terminals determine the PIDs used for the IPoS logical channels by reading the two PSI tables, table 4.9.2-1 and table 4.9.2.-2:

- The Program Association Table (PAT) gives the PID of the Program Map Table (PMT).

- The PMT determines the PIDs of the various logical channels used in IPoS.

IPoS terminals shall be capable of receiving the PIDs in table 4.9.2-1

Table 4.9.2-1. PID Range

Description	PID (hex)
Program Association Table	0x0000
Program Map Table	From 0x0010 to 0x1FFE as defined in the PAT
IPoS Outroute Logical Channels	From 0x0010 to 0x1FFE as defined in the PMT

IPoS terminals are configured through the PAT with PID value 0x0000, which determines the PMT table's PID. Then, through the PMT table, the PIDs to use for IPoS-specific logical channels are determined.

When PAT and PMT tables are not present in the outroute carrier, the default values in table 4.9.2-2 are used for the IPoS specific logical control channels.

Table 4.9.2-2. IPoS Default PIDs

Description	PID (hex)
IPoS Logical Control Channels	0x0190
IPoS Logical Traffic Channels	0x012C

4.10 Outroute MAC Sublayer

The purpose of the MAC sublayer is to provide higher layer information with access to the transmission services from the multiplexing sublayer and the physical layers. The outroute MAC sublayer performs the following functions:

- Mapping of higher layer information into MPEG packets defined at the multiplexer sublayer
- Addressing individual, group, or all IPoS terminals receiving the outroute carrier
- Logical channel definition and control of information flows over the various channels
- Detection of transmission errors introduced over the air interface

4.10.1 Outroute MAC Formats

The MAC sublayer maps higher layer information over the 184-byte payload of the DVB/MPEG packets using MAC layer delimiters designated as MAC headers and trailers. Two types of MAC formats are defined in the outroute direction:

1. The format associated with the PIDs containing PSI tables that enable the configuration of the DVB/MPEG multiplex with several programs.
2. The MAC format for IPoS information forwarded through IPoS-defined logical channels.

4.10.1.1 PSI Table Format

PSI tables are broadcast over the outroute carrier to enable the configuration of IPoS and non-IPoS terminals to the various programs that might exist in the outroute multiplex.

The encapsulation of PSI tables used to configure the IPoS terminals over the outroute transport stream complies with the definition for SI tables in reference [1] (found in subsection 1.4 of this document). This encapsulation is made according to the following rules:

- PSI tables may be segmented into one or more sections before being inserted into the transport packets.
- Sections are of variable length. The maximum length of the section is 1024 bytes (including the section header and CRC).
- Each section may start at the beginning of the payload of an MPEG packet and span for one or more packets.
- The transport packet payload for PSI segments or tables contains an 8-bit pointer field following the 4-byte DVB/MPEG header as defined in subsection 4.9. The pointer field indicates the number of bytes following the pointer-field until the beginning of the MAC PDU in the first DVB/MPEG packet, e.g., a value of 0x00 in the pointer_field, indicates that the section starts immediately after the pointer_field.

Figure 4.10.1.1-1 shows the segmentation of tables into multiple sections, the formatting of each section into one MAC PDU, and the encapsulation of the MAC PDUs into the payload of one or more transport packets.

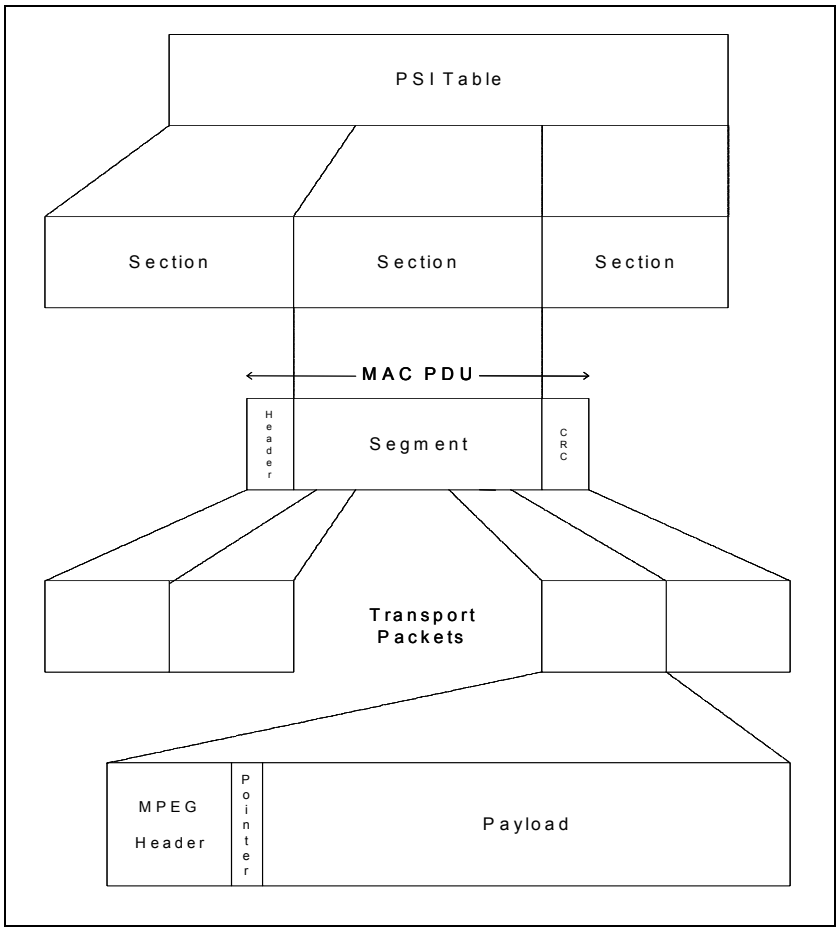


Figure 4.10.1.1-1. MAC Encapsulation of PSI Tables

The payload of the transport packets for PSI segments or tables contains the 8-bit pointer_field following the 4-byte DVB/MPEG transport header as defined in subsection 4.9.1. The pointer_field value indicates the number of bytes following the pointer_field until the beginning of the MAC PDU in the first packet, e.g., a value of 0x00 in the pointer_field indicates that the section starts immediately after the pointer_field.

The MAC PDU for PSI sections or tables includes the following elements:

- A 64-bit section header
- The PSI table/section content
- A 32-bit section trailer or CRC-32

4.10.1.1.1 SI Section Header

The 64-bit long section header for PSI sections is formatted according to the structure defined for SI in reference [1] (found in subsection 1.4 of this document). The fields in the section header are defined in table 4.10.1.1.1-1.

Table 4.10.1.1.1-1. SI Section Header

Field Name	Field Length (bits)
table_id	8
section_syntax_indicator	1
reserved_for_future_use	1
reserved	2
section_length	12
network_id	16
reserved	2
version_number	5
current_next_indicator	1
section_number	8
last_section_number	8

The description of the fields and of their values in the section header is as follows:

- table_id: This field identifies the type of table as follows:
  - PAT 0x00
  - PMT 0x02
- section_syntax_indicator: Set to '1'. This indicates that the entire structure of the table header shall be used.
- reserved_for_future_use: Set to '0'.
- reserved: Set to '11'.
- section_length: The first two bits in this 12-bit field are set to '00'. The remaining 10-bit subfield specifies the number of bytes in the section, including the section header and the CRC.
- network_id: This is a 16-bit field serving as a label to identify the particular IPoS network to which the table shall apply.
- Reserved: Set to '11'.
- version_number: This 5-bit field is the version number of the table. The version_number shall be incremented by 1, module 32, whenever the information carried within the table changes. When the current_next_indicator is set to '1', then the version_number shall be that of the currently applicable table. When the current_next_indicator is set to '0', then the version_number shall be that of the next applicable table.
- current_next_indicator: A 1-bit indicator, when set to '1' indicates that the table is currently applicable. When the bit is set to '0', it indicates that the table sent is not yet applicable and shall be the next table to be valid.

- section_number: This 8-bit field gives the number of the section. The section_number of the first section in the table shall be '0x00'. The section_number shall be incremented by 1 with each additional section with the same table_id and network_id.

- last_section_number: This 8-bit field specifies the number of the last section (that is, the section with the highest section_number) of the table of which this section is a part.

4.10.1.1.2 PSI Table/Sections

PSI tables and sections provide the information that permits configuration of the IPoS terminals to the logical channels included in the outroute carrier. The IPoS PSI data is included in two tables designated as:

- Program Association Table: The PAT_PID is 0x0000. The PAT indicates the correspondence between program numbers and the PID values of the transport stream that carries this information.

- Program Map Table: The PMT_PID is listed in the PAT. The PMT contains a list of all the IPoS-specific logical channels.

The content of the PSI tables is structured with DVB-standard data broadcast descriptors defined in references [11] and [12] (found in subsection 1.4 of this document).

4.10.1.1.3 IPoS Data Broadcast Service Descriptor

The IPoS service shall be indicated with a data broadcast descriptor with the fields in table 4.10.1.1.3-1.

Table 4.10.1.1.3-1. Outroute IPoS Data Broadcast Descriptor

Field Name	Field Length (bits)
data_broadcast_id	16
component_tag	8
selector_length	8
MAC_address_range	3
MAC_IP_mapping_flag	1
alignment_indicator	1
reserved	3
max_sections_per_datagram	8

The description of the IPoS data broadcast descriptor's fields and values is as follows:

- data_broadcast_id: Set to 0x0005 to indicate the use of multiprotocol encapsulation.

- component_tag: This field has the same value as a component_tag field of a stream_identifier_descriptor that may be present in the PSI program map section for the stream on which the data is broadcast. If this field is not used, it shall be set to value 0x00.

- selector_length: Set to 0x02. Indicates the length of the following fields in the descriptor.

- MAC_address_range: Set to 0x06. Indicates the number of MAC address bytes used in the service.

- MAC_IP_mapping_flag: Set to '1'. Indicates the type of mapping between IP to MAC addresses.

- alignment_indicator: Set to '1'. Indicates that the alignment between the datagram_section and the transport stream is 32 bits.

- reserved: Set to '111'.

- max_sections_per_datagram: Set to 0x01. Indicates the maximum number of sections that can be used to carry a single datagram unit.

4.10.1.1.4 Section Trailer

This field contains a 32-bit CRC (CRC-32) as described in reference [1] (found in subsection 1.4 of this document). The CRC is calculated with the following polynomial:

$$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^{8} + x^{7} + x^{5} + x^{4} + x^{2} + x^{1} + 1$$

The 32-bit CRC decoder operates at the bit level, a typical implementation of the decoder is shown in figure 4.10.1.1.4-1.

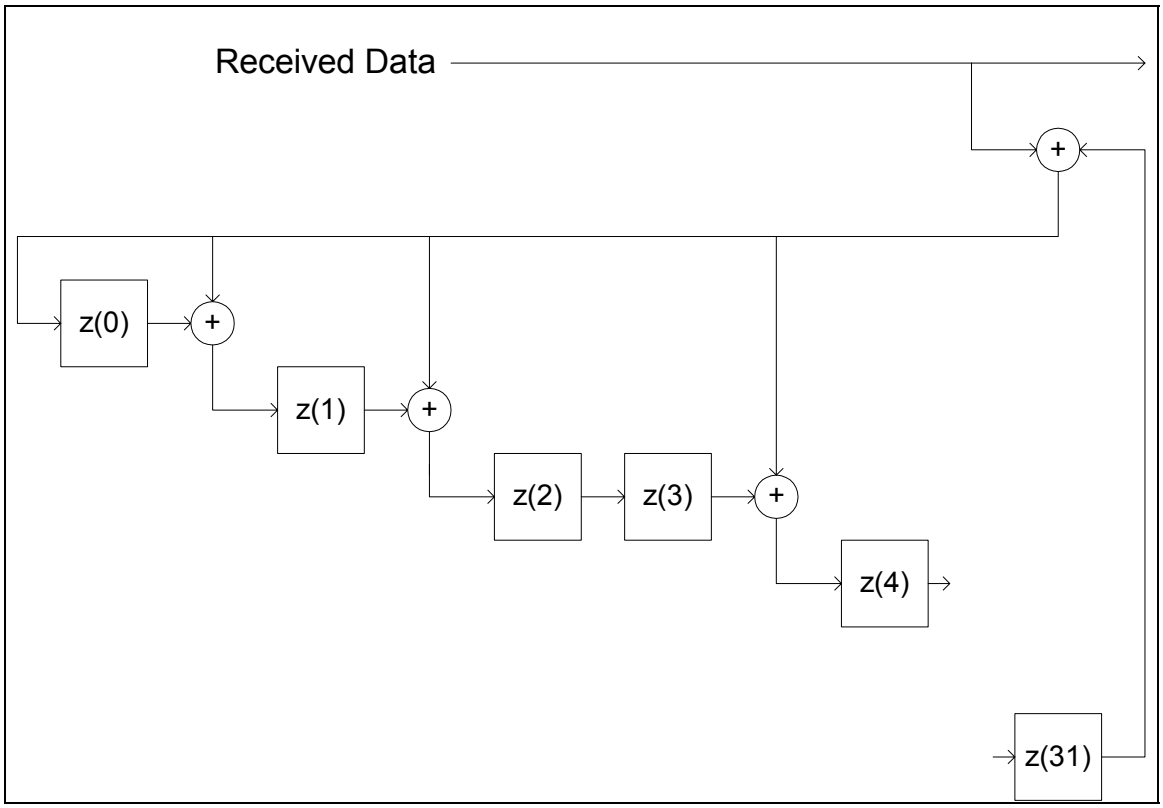


Figure 4.10.1.1.4-1. DVB/MPEG-2 Transport Packet CRC-32 Decoder

The following steps describe the operation of the DVB/MPEG-2 transport packet CRC-32 decoder:

- Before CRC processing, each delay element z (i) is set to its initial value '1'.
- The MAC PDU, including header, section, and 32-bit CRC, is received with the first transmitted byte and its MSB first.
- After shifting the last bit of the CRC-32 into the decoder, e.g., into z (0) after the addition of the output of z (31), the output of all delay elements is read.
- In the case where there are no errors in the MAC PDU, each of the outputs of z (i) shall be zero.

4.10.1.2 IPoS MAC Formats

The MAC formats in this subsection define the mapping of IPoS specific control and user information over the DVB/MPEG-2 transport streams provided by the multiplexing sublayer. Within the IPoS specific outroute logical channels, the same MAC format is used for user traffic and control messages, independent of whether they are delivered in unicast, multicast, or broadcast connectivity.

IPoS control and user information are mapped into the DVB/MPEG transport streams using a MAC format based on the DVB data broadcasting multiprotocol encapsulation profile for the encapsulation of IP datagrams described in reference [12] (found in subsection 1.4 of this document). The IP datagrams might, in turn, encapsulate a network layer transport protocol such as TCP or UDP, as well as IPoS control messages. This encapsulation is made according to the following rules:

- The outroute MAC sublayer passes the datagrams without any fragmentation. The entire datagram is contained in a single MAC PDU.
- The MAC PDU containing the datagram starts at the beginning of the payload of an MPEG packet and may span for one or more packets.
- Datagrams are variable length. Stuffing bytes, 0xFF, are used when necessary to complete the payload of the last packet in the transport stream.

Figure 4.10.1.2-1 shows the encapsulation of datagrams containing IPoS user or control information into a single MAC PDU without segmentation, and the encapsulation of the MAC PDUs into the payload of one or more transport packets. The boundaries of the higher layer datagrams are preserved by delimiters and the stuffing bytes defined at the MAC sublayer.

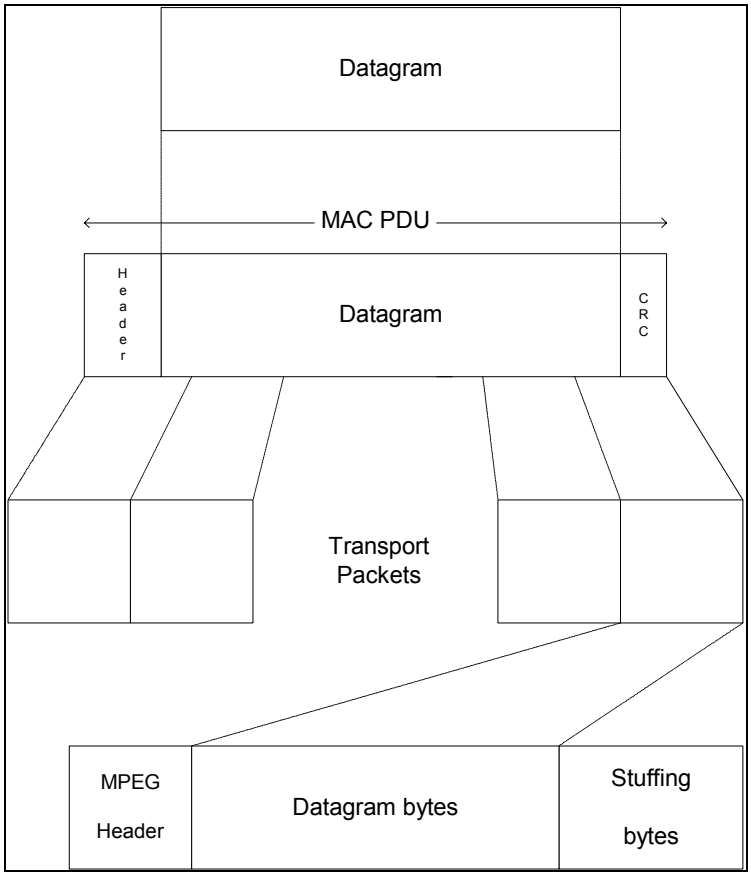


Figure 4.10.1.2-1. MAC Encapsulation of Datagrams

IPoS outroute MAC format includes the following elements:

- A 96-bit MAC header
- The MAC payload with a datagram containing the IP packet or control message
- The 32-bit trailer field

The routing of information to IPoS terminals is based on the address field included in the 96-bit MAC header. This MAC addressing is different from the program addressing provided by the PID field in the DVB/MPEG packet.

4.10.1.2.1 IPoS MAC Header

The 96-bit IPoS MAC header is formatted according to the multiprotocol encapsulation profile in references [12] and [13] (found in subsection 1.4 of this document). The fields in the outroute IPoS MAC header are defined in table 4.10.1.2.1-1.

Table 4.10.1.2.1-1. Outroute MAC Header

Field Name	Field Length (bits)
table_id	8
section_syntax_indicator	1
private_indicator	1
reserved	2
section_length	12
MAC_address_6	8
MAC_address_5	8
reserved	2
payload_scrambling_control	2
address_scrambling_control	2
LLC_SNAP_flag	1
current_next_indicator	1
section_number	8
last_section_number	8
MAC_address_4	8
MAC_address_3	8
MAC_address_2	8
MAC_address_1	8

The outroute MAC header contains the following values:

- table_id: Set to 0x3E. Indicates DSM-CC sections with private data.
- section_syntax_indicator: Set to '1'. Indicates the use of CRC-32 as the trailer to the MAC PDU.
- private_indicator: Set to '0'. Indicates that IPoS uses CRC-32.

- reserved: Set to '11'.
- section_length: Set to the number in bytes in the section starting immediately following the section_length field through the CRC-32 inclusive.
- MAC_address: This 48-bit field contains the MAC address of the destination; see subsection 4.10.1.3.
- reserved
- payload_scrambling_control: This 2-bit field defines the encryption mode of the payload section. This includes the payload starting after the MAC_address_1 but excludes the CRC-32 field. The IPoS outroute utilizes the payload_scrambling_control field to indicate whether the payload is encrypted or not. IPoS utilizes the following payload_scrambling_control field values:

  0x00 - unencrypted
  0x01 - not used
  0x02 - encrypted with even-numbered traffic-key version
  0x03 - encrypted with odd-numbered traffic-key version

- address_scrambling_control: Set to '00'. This 2-bit field defines the scrambling mode of the MAC address section as unencrypted.
- LLC_SNAP_flag: Set to '0'. Indicates that the payload does not use LLC/SNAP encapsulation.
- current_next_indicator: This 1-bit field shall be set to '1'.
- section_number: Set to 0x00. Indicates IPoS does not use fragmentation of IP packets in the outroute direction.
- last_section_number: Set to 0x00. Indicates IPoS does not use fragmentation of IP packets in the outroute direction.

4.10.1.2.2 MAC Payload

The MAC payload contains a datagram with the IP packet or control message. The encapsulation of the payload between the MAC header and the trailer is described in table 4.10.1.2.2-1.

Table 4.10.1.2.2-1. Outroute IPoS MAC PDU Format

Field Name	Field Length (bytes)	Comments
Header	12	
Initialization Vector	7	This field only exists when encryption is enabled.
Sequence Number	1	This field only exists when encryption is enabled.

Table 4.10.1.2.2-1. Outroute IPoS MAC PDU Format

Field Name	Field Length (bytes)	Comments
Datagram Bytes	N1	
Padding Bytes	1-to-3	Pad the datagram to an encryption boundary.
CRC-32	4	

The description of the fields in the outroute payload is the following:

- Initialization vector: A 7-byte field that providing the initialization input to the DES encryption module used to ensure that outroute information is only accessible to authorized users.

- Sequence Number: The first two bits of this 8-bit field contain the packet priority (the value '00' representing the lowest priority, and the value '11' the highest). The remaining 6 bits provide a sequence number that is incremented by a value of one from the previous sequence number for the same MAC address transmitted in all outroute logical channels with the exception of the conditional unicast and multicast access channels. On the outroute conditional channels, the sequence number is set to '000000'. The remote terminals use the sequence number to detect packet losses.

- Datagram bytes: This field includes the bytes of the outroute datagram without segmentation.

- Padding bytes, 0xFF bytes, are added to make the packet a multiple of encryption words. The padding to the encryption boundary takes place regardless of the content of the payload_scrambling_control field. The padding bytes are encrypted if indicated by the payload_scrambling_control field.

4.10.1.2.3 MAC Trailer

This field contains the CRC-32 described in subsection 4.10.1.1.4 to verify the integrity of the outroute transmission.

4.10.1.3 MAC Addressing

The 96-bit MAC header in the multiprotocol encapsulation profile defines a 48-bit MAC_address field that is used to convey the IPoS MAC address used to deliver user traffic and control messages to the appropriate IPoS terminal. The MAC_address field in the header is fragmented in six fields of 8 bits labeled MAC_address_1 to MAC_address_6.

The IPoS MAC addresses are also 48 bits long, and they are represented by a string of 6 bytes, six pairs of hexadecimal digits, with each byte separated by a space (for example 00 02 AE 6C 77 9B). IPoS MAC addresses comply with reference [14] (found in subsection 1.4 of this document). In the IPoS MAC

addresses, the bytes are displayed left to right in the order in which they are transmitted. Bit 0 of the address is bit 0 of the first byte. Bit 47 of the address is bit 7 of the 6th byte.

The DVB Specification for data broadcasting's multiprotocol encapsulation profile calls for the bytes within a MAC address to appear in the opposite order that they appear within the Ethernet frame in reference [14] (found in subsection 1.4 of this document). The order in which the IPoS MAC address appears in the MAC header is shown in figure 4.10.1.3-1; the order of the bits within the byte does not change.

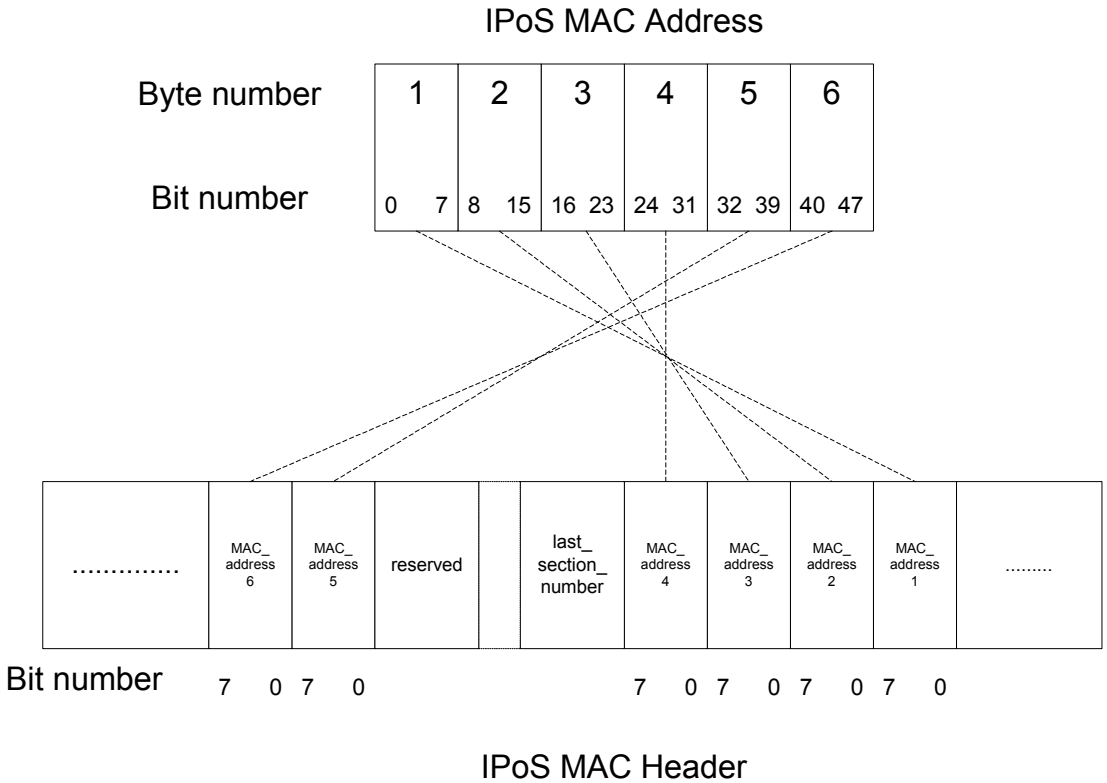


Figure 4.10.1.3-1. IPoS MAC Address to MAC Header Mapping

The MAC_address_1 field contains the MSB of the IPoS MAC address, while MAC_address_6 contains the LSB of the IPoS MAC address.

IPoS MAC addresses take different forms depending on the type of traffic and the number of IPoS terminals associated to the MAC addresses. IPoS supports the following MAC addressing modes:

- Unicast
- Multicast
- Superframe Numbering
- Return Broadcast

- Return Group
- Unicast Conditional Access
- Multicast Conditional Access

4.10.1.3.1 Unicast Addressing

Unicast MAC addresses are used in all user traffic to and from each individual IPoS terminal or PC. Unicast MAC addresses are similar to a private Ethernet address on a LAN port.

Each IPoS terminal or PC is configured with one unicast MAC address. This IPoS unicast MAC address is related to the serial number of the IPoS terminal. The serial number of the IPoS terminal is loaded into the terminal at the factory. Serial numbers are unique within the particular IPoS system.

The unicast IPoS MAC address is determined by the IPoS terminal serial number. The low-order 24 bits of the serial number are placed into the three high-order bytes of the MAC address. The mapping of the serial number to fields of the unicast address is shown in table 4.10.1.3.1-1.

Table 4.10.1.3.1-1. Unicast MAC Address

MAC Address Bits	MAC Header field	Description
40-47	MAC_address_6	Holds bits 0…7 of the serial number unique to each IPoS terminal
32-39	MAC_address_5	Holds bits 8…15 of the serial number
24-31	MAC_address_4	Holds bits 16…23 of the serial number
16-23	MAC_address_3	Set to 0x0A
8-15	MAC_address_2	Set to 0x00
0-7	MAC_address_1	Set to 0x02, defining that the address is a unicast address

Examples of IPoS unicast addresses are given in table 4.10.1.3.1-2.

Table 4.10.1.3.1-2. IPoS Unicast MAC Address Examples

Address Type	IPoS Terminal Serial Number	MAC Address (Hex)
IPoS Unicast Address	Serial Number 1	02 00 0A 00 00 01
	Serial Number 256	02 00 0A 00 01 00

4.10.1.3.2 Multicast Addressing

IPoS multicast addresses are used to transport user information to groups of IPoS terminals or PCs receiving the same outroute carrier. The IPoS multicast addresses are determined from multicast addresses compliant with reference [15] (found in subsection 1.4 of this document).

A MAC multicast address is obtained by mapping the low-order 23 bits of the IPoS multicast address into the three high-order bytes of the multicast MAC address. Since the IPoS multicast address has 28 significant bits and only 23 bits are mapped to the MAC address, more than one IPoS multicast address may map to the same MAC multicast address. Care should be taken to ensure that multiple IPoS addresses that map to the same MAC address are not used within the IPoS system.

The fields of the multicast address are shown in table 4.10.1.3.2-1.

Table 4.10.1.3.2-1. Multicast MAC Address

MAC Address Bits	MAC Header Field	Description
40-47	MAC_address_6	Holds bits 0…7 of the IP address.
32-39	MAC_address_5	Holds bits 8…15 of the IP address.
24-31	MAC_address_4	Holds bits 16…22 of the IP address. Bit 7 of this byte is zero.
16-23	MAC_address_3	Set to 0x5E
8-15	MAC_address_2	Set to 0x00
0-7	MAC_address_1	Set to 0x01, indicating that the address is a multicast address.

Examples of multicast addresses are given in table 4.10.1.3.2-2.

Table 4.10.1.3.2-2. IPoS Multicast MAC Address Examples

Address Type	Multicast Address	MAC Address (Hex)
IPoS Multicast Address	225.2.3.4	01 00 5E 02 03 04
	239.221.204.1	01 00 5E 6D CC 01

The value 0x01 in the first byte of the MAC address indicates the multicast nature of the address.

4.10.1.3.3 Superframe Numbering Address

The superframe numbering address is a dedicated broadcast address used by a special IPoS channel that allows IPoS terminals to distinguish the network to which they are connected and to obtain timing information needed for inroute transmissions.

The Superframe Numbering address is given in table 4.10.1.3.3-1

Table 4.10.1.3.3-1. IPoS Superframe Numbering Address

Address Type	MAC Address (Hex)
Superframe Numbering	03 00 01 02 00 00

The value 0x03 in the first byte of the MAC address indicates the broadcast nature of the address.

4.10.1.3.4 Return Broadcast Address

The return broadcast address is used for control messages that must be received by all IPoS terminals on specific transponders. The IPoS return broadcast address is given in table 4.10.1.3.4-1.

Table 4.10.1.3.4-1. IPoS Return Broadcast MAC Address Examples

Address Type	MAC Address (Hex)
IPoS Return Broadcast	03 00 01 01 00 00

4.10.1.3.5 Return Group Addressing

Return group addresses are used for messages sent to one specific group of IPoS terminals that are assigned to this group. The return group addresses are also monitored by IPoS terminals that were activated on that inroute group or are considering becoming active on that inroute group. The grouping is implemented to provide a scalable approach of forwarding information so that a single IPoS terminal does not need to process all the return group addresses in the system.

Examples of return group address are given in table 4.10.1.3.5-1.

Table 4.10.1.3.5-1. IPoS Return Group MAC Address Examples

Address Type	Group Number	MAC Address (Hex)
IPoS Return Group	Group 1	03 00 01 00 00 01
	Group 2	03 00 01 00 00 02

4.10.1.3.6 Unicast Conditional Access

The hub uses unicast conditional access addresses to send control messages, designated as conditional access information, to individual IPoS terminals. Conditional access information, e.g., decryption keys, permits IPoS terminals to access different multicast streams.

The MAC unicast conditional access addresses are identical to the unicast traffic MAC address. Examples of unicast conditional access addresses are given in table 4.10.1.3.6-1.

Table 4.10.1.3.6-1. IPoS Unicast Conditional Access MAC Address Examples

Address Type	IPoS Terminal Serial Number	MAC Address (Hex)
IPoS Unicast Conditional Access	Serial number 1	02 00 0A 00 00 01
	Serial number 256	02 00 0A 00 01 00

4.10.1.3.7 Multicast Conditional Access

The hub uses multicast conditional access addresses to send conditional access information to a group of IPoS terminals. The MAC multicast conditional access addresses are identical to the multicast traffic MAC addresses. An example of a multicast conditional access address is given in table 4.10.1.3.7-1.

Table 4.10.1.3.7-1. IPoS Multicast Conditional Access Address Examples

Address Type	Multicast Address	MAC Address (Hex)
IPoS Multicast Conditional Access	225.2.3.4	01 00 5E 02 03 04
	239.221.204.1	01 00 5E 6D CC 01

4.10.1.4 Outroute Logical Channels

This subsection describes the formats in the logical channels used for forwarding IPoS specific control and user information from the hub to the IPoS terminals and their associated PCs.

Logical channels are defined by the type of information and the addressing associations made among the access points to the MAC layer and the IPoS terminals receiving the information. The definition of logical channels isolates the higher layer's delivery of information from the peculiarities of the MAC and PHYs.

Outroute logical channels are identified by the PID in the multiplexing sublayer and the IPoS MAC address that indicates the type and destination of the information.

According to the submultiplexer PID, IPoS logical channels are divided into:

- Traffic channels
- Control channels

MAC addressing defines three types of connectivity for the logical channel:

1. Point-to-point connections, defined with a unicast address, to deliver information to a single IPoS terminal
2. Point-to-multipoint connections, defined with a multicast address, to deliver the same information to a group of IPoS terminals

3. Broadcast connectivity to deliver the same information to all IPoS terminals in the system

Table 4.10.1.4-1 provides a list of logical channels with examples of their corresponding MAC and multiplexing layer addresses.

Table 4.10.1.4-1. Classification of IPoS Logical Channels

Type of Channel	Logical Channel Designation	MAC Address	PID (default)
Traffic	Unicast traffic	02 00 XX XX XX XX	0x0004
Traffic	Multicast traffic	01 00 5E XX XX XX	0x0004
Control	Superframe Numbering Broadcast	03 00 00 00 00 02	0x0003
Control	Return Broadcast	03 00 00 00 00 01	0x0003
Control	Return Group	03 00 01 00 XX XX	0x0003
Control	Unicast conditional access	02 00 XX XX XX XX	0x0003
Control	Multicast conditional access	01 00 5E XX XX XX	0x0003

User information and control messages are embedded inside the datagram section of the outroute MAC format as described in the following subsections. The routing and filtering of packets at the receiving IPoS terminal are made based on the PID and the MAC addresses.

The control messages format has been defined to be implemented easily and is flexible enough to accommodate the future signaling needs of the IPoS system. The first byte, the Frame_type field, in all control message formats identifies the particular message.

4.10.1.4.1 Unicast Traffic Channels

Unicast traffic channels transport user traffic and IP datagrams inside the datagram_section of the IPoS MAC structure. The targeted individual IPoS terminal is designated in the unicast traffic address in the MAC header.

The content of the datagram_section following the MAC header depends on whether or not scrambling is enabled in the IPoS MAC header.

If scrambling is enabled, then the first 8 bytes immediately following the MAC header contain:

- Initialization vector, first 7 bytes of the payload. This field is used for the decryption of the datagram.
- Sequence number, byte eight of the payload. This field is specific to each IPoS terminal and is used to determine the packet priority and detect out-of-sequence packets.

If scrambling is disabled, the IP datagram, including the IP header and payload, immediately follow the MAC header.

4.10.1.4.2 Multicast Traffic Channels

Multicast traffic channels are used for the distribution of multicast streams to groups of authorized IPoS terminals. The multicast information is conveyed to those groups of PCs inside the datagram section of MAC PDUs identified in the multicast address in the MAC header.

The hub distributes a list of keys for multicast traffic periodically. If the IPoS terminal is enabled to receive the multicast address, then the IPoS terminal will enable the appropriate IP multicast MAC addresses it is authorized to receive.

4.10.1.4.3 Superframe Numbering Channel

This channel provides a timing reference and identification for the satellite transponder over the dedicated MAC superframe numbering address. Only one type of control message, designated the Superframe Numbering Packet (SFNP), is carried in this channel.

Two SFNPs are sent by the hub every 360 msec for redundancy purposes. IPoS terminals shall have separate state machines to track the two SFNPs. Only one SFNP will actively control timing, but the IPoS remote will be able to transition to the other SFNP when necessary.

The following rules shall be used in processing the SFNP at the IPoS terminals:

- No transmission will be allowed if the IPoS terminal PHY is not synchronized; this will not affect the IPoS remote's ability to acquire network timing.

- Both SFNPs will be monitored, if present, but a change in selection will be made only after receiving three consecutive valid SFNPs from the same source.

- Network timing is declared as in-sync only after receiving three consecutive valid SFNPs from a timing source and having the local timing match within eight clock cycles of the 10 MHz clock reference used at the hub to generate the timing of the SFNPs. This will typically require four superframe times.

- Network timing is declared as out of sync after receiving two consecutive SFNPs from the selected timing source and having the local timing off by more than 16 clocks.

- Network timing is declared as out of sync and the network timing source becomes unselected after not receiving any SFNPs for three superframe times.

- Network timing is declared as out of sync and the network timing source becomes unselected after not receiving two consecutive SFNPs for five superframe times.

- Network timing is declared as out of sync and the network timing source becomes unselected after not receiving three consecutive SFNPs for seven superframe times.

4.10.1.4.4 Return Broadcast

This logical channel is used to distribute control messages to all IPoS terminals. The following control messages are transmitted over this channel:

- Inroute Group Definition Packet (IGDP). This message defines available return channel groups and resources available on each group.

- Inroute Command/Ack Packet (ICAP). This message contains a list of commands to be sent to the IPoS terminal from the hub.

4.10.1.4.5 Return Group Logical Channels

The return group logical channels are used for control messages sent to specific IPoS terminals assigned to a group. The return group logical channels are also monitored by IPoS terminals that were recently active on that inroute group or are considering becoming active on that inroute group. The grouping is implemented to provide a scalable approach to transmitting control messages.

The message types received over the return logical channels are:

- Bandwidth Allocation Packet (BAP): This message contains the bandwidth allocation and the allocation of the bursts to each IPoS terminal in the group.

- Inroute Acknowledgment Packet (IAP): This message contains a bitmask indicating which bursts in the frame were successfully received at the hub.

- Inroute Command/Ack Packet (ICAP): This message contains a list of commands and explicit acknowledgments sent to IPoS terminals from the hub.

It is important to note that if an inroute group advertises that it has Aloha or unallocated ranging bursts, the inroute group must have some number of those bursts defined every frame for the next 10 frames. Furthermore, the number of bursts should be evenly spread across all frames in the superframe. Failure to meet this requirement will result in higher collision rates and increased user latency.

4.10.1.4.6 Unicast Conditional Access Channel

Unicast conditional access channels are used by the hub to send periodic control messages containing decryption keys and other conditional access information to specific IPoS terminals with enabled MAC addresses. The rate at which the Conditional Access messages are sent is controlled by parameters in the hub.

Only one type of command, designated Periodic Adapter Conditional Access Update (PACAU), is sent over this channel.

4.10.1.4.7 Multicast Conditional Access Channel

Over this channel, the hub sends periodic control messages containing mappings of multicast keys to the list of multicast MAC addresses included in the PACAU.

Only one type of command-designated Periodic Element Broadcast (PEB) is sent over this channel. PEB commands are sent continuously to support relatively quick notification in the event of a key change and/or the addition of new IPoS terminals.

4.11 Inroute MAC Sublayer

The inroute in IPoS is significantly different from the outroute direction because of the need to optimize transmission over highly asymmetric satellite links. The inroute MAC adapts user and control information into generic byte-oriented streams that map the higher order information into the TDMA frame format defined by the IPoS PHY over the inroute direction.

The information from individual IPoS terminals to the hub over the inroute channels is structured as one or more MAC PDUs. Each MAC PDU is transmitted over the payloads of a block of consecutive slots associated to a time interval defined by the inroute bandwidth allocation procedure. Each assigned interval consists of a sequence of slots within the multifrequency TDMA structure defined at the PHY.

Figure 4.11-1 illustrates the segmentation and encapsulation of higher order information, through the inroute protocol layers to the payload of the TDMA bursts, defined at the PHY.

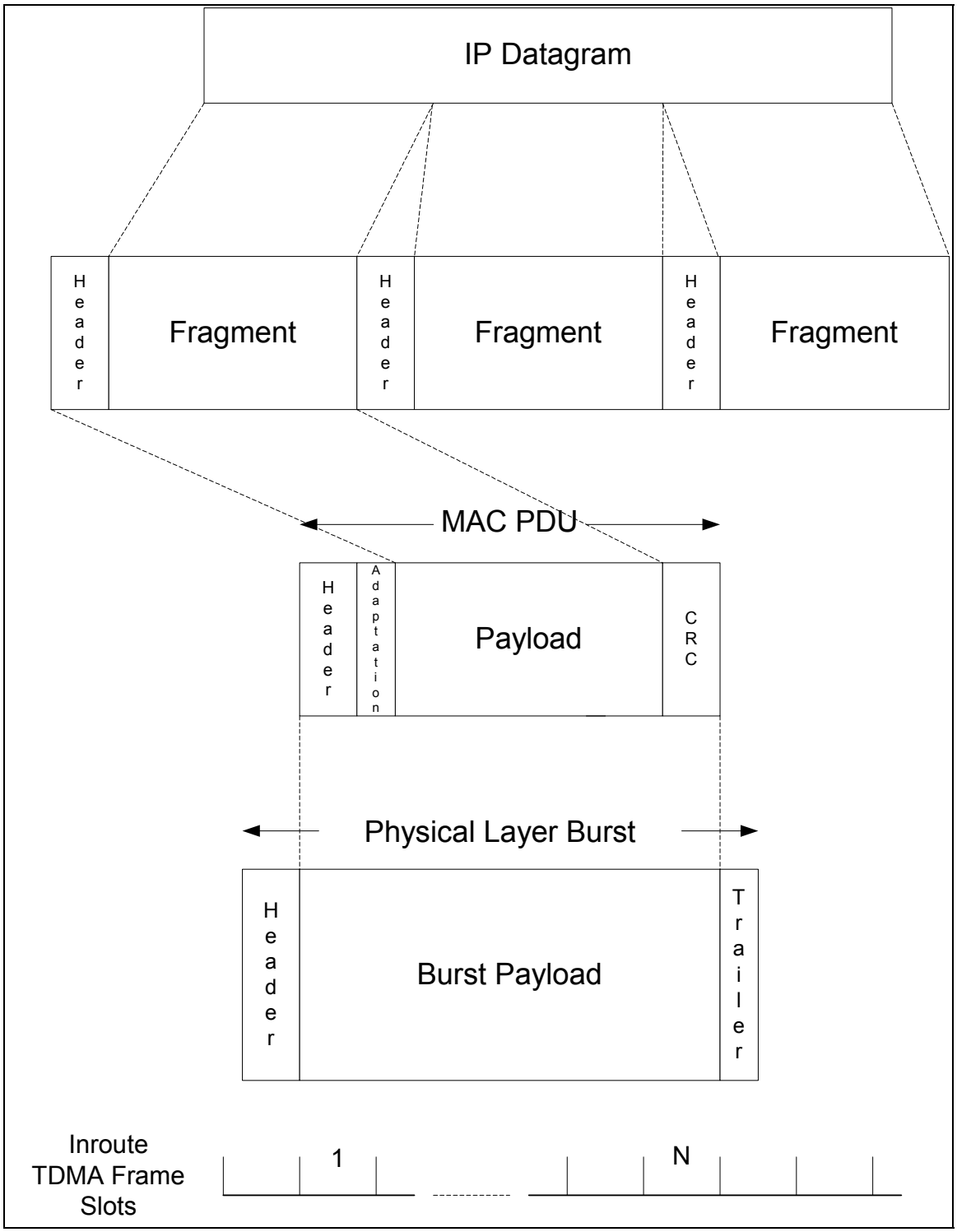


Figure 4.11-1. Inroute MAC Encapsulation of Datagrams

User level IP datagrams are segmented at the input of the IPoS terminal DLC into one or more MAC PDUs, or datagram fragments, which are buffered until successfully transmitted over the inroute link. The inroute MAC layer encapsulates the information to be transmitted into the byte stream formed by the payload of the bursts transmitted by the IPoS remote.

Proper recovery of the inroute information at the hub requires a reliable, in order, processing of the payload of the group of bursts used to transmit the IP datagram. To resolve problems due to data loss on the inroute, the SLC provides an acknowledgment procedure.

The combined payload size of each of the bursts transmitted by the IPoS remote varies with the number of effective slots, N, used in the inroute transmission, the transmission rate, and FEC encoding in the inroute carrier. The payloads defined by the PHY for the different types of bursts are given in table 4.11-1

Table 4.11-1. Burst Payloads

Burst Type	Payload Size (Bytes)
64 ksps convolutional	7*N
128 ksps convolutional	8*N
256 ksps convolutional	9*N
128 ksps Turbo	9*N
256 ksps Turbo	9*N

4.11.1 Inroute Logical Channels

Two logical channel types are defined in the inroute direction:

1. Unallocated channels: These are slots or groups of slots designated to be shared by multiple IPoS terminals using a random access procedure. The unallocated channels are primarily used for control messages in the inroute direction. Piggybacking of user data with control messages is supported in the Aloha channels.

2. Allocated channels: These are slots or a sequence of slots in an allocated time interval that are dedicated to one specific IPoS terminal for the transmission of user information.

The following subsections define the MAC structures for both types of logical channels.

4.11.1.1 MAC Formats for Unallocated Channels

The unallocated channels are used to transfer control messages in the inroute direction. IPoS terminals send two control messages over the unallocated logical channels:

1. Bandwidth Allocation Request (BAR)
2. Ranging Request

The MAC structures used over the unallocated logical channels consist of four sections:

1. MAC header
2. Adaptation field
3. Payload or datagram bytes
4. Trailer field

The encapsulation of the datagram in the inroute MAC PDU for unallocated channels is shown in table 4.11.1.1-1.

Table 4.11.1.1-1. Inroute MAC PDU Format

Field Name	Field Length (Bytes)	Comments
Header	6 or 9	6 bytes for Turbo coding, 9 bytes for convolutional coding
Adaptation	0 to M	
Payload	N	
CRC-16	2	

The MAC Header format varies depending on whether the coding used in the PHY is convolutional or Turbo encoding. Also, the inroute MAC structure might include an Adaptation field that is used to convey management information to the hub.

4.11.1.1.1 MAC Header for Unallocated Channels with Convolutional Coding

The 72-bit MAC Header for sending either BARs or Ranging Requests over the inroute unallocated channels using convolutional coding is shown in table 4.11.1.1.1-1.

Table 4.11.1.1.1-1. MAC Header for Convolutional Coding (Unallocated)

Field Name	Field Length (Bits)
SerNr_low	8
Backlog_indicator	1
Adaptation_indicator	1
Frame_number	2
BurstNr	4
Length_FEC	8
Length	8
SerNr_high	18

Table 4.11.1.1.1-1. MAC Header for Convolutional Coding (Unallocated)

Field Name	Field Length (Bits)
Version	2
Reserved	4
Backlog	16

The description of the fields in the MAC header for convolutional encoding is the following:

- SerNr_low: This field contains the 8 LSBs of the IPoS terminal's serial number.
- Backlog_indicator: This flag indicates the presence of the backlog; the field is set to '1' to indicate the presence of backlog. Backlog is always present for BARs or Ranging Request unless there is no backlog.
- Adaptation_indicator: This field indicates the presence/absence of the Adaptation field. Set to '0' to indicate that the Adaptation field is present.
- Frame_number: This field contains the frame number's 2 LSBs. This field helps the hub determine which burst was received.
- BurstNr: This field indicates the slot in the frame in which this burst was transmitted.
- Length_FEC: This field indicates the FEC value for the burst length.
- Length: This shall be the length of the burst. It includes all the bytes, starting with the Backlog_indicator field through the CRC.
- SerNr_high: This field contains the MSBs of the IPoS terminal's serial number.
- Version: This field identifies the version of the protocol. The use of version numbers allows future message changes. The specifications in this document are version 1.
- Reserved: Set by the IPoS terminal as 0.
- Backlog: This 2-byte field supports prioritized backlog information. The first byte provides the total backlog in bytes; it is encoded as a floating point number with a 2-bit exponent field and a 6-bit mantissa and shall be rounded up by the IPoS terminal. The backlog shall be indicated by

$$8^{\text{Backlog}[7:6]} \times \text{Backlog}[5:0] \times 2.$$

This shall yield an even number up to 64K, which is the maximum practical queue size to be tracked since this will fully occupy a 256 ksps inroute for 2 seconds. The second byte shall contain the highest priority for which there is a backlog in the two high-order bits, and the remainder

of the byte identifies the percentage (of the backlog that belongs to the priority indicated by the two higher-order bytes) in 1/64 units (the value is ((n+1)/64)*backlog where "n" is the number provided).

4.11.1.1.2 MAC Header for Unallocated Channels with Turbo Coding

The 48-bit MAC header used with Turbo coding, 3 bytes shorter than the MAC header for convolutional coding, is shown in table 4.11.1.1.2-1.

Table 4.11.1.1.2-1. MAC Header for Turbo Coding (Unallocated)

Field Name	Field Length (Bits)
Backlog_indicator	1
Adaptation_indicator	1
Version	2
Reserved	1
Adaptation_Length	1
Serial_number	26
Backlog	16

The description of the fields in the MAC header for Turbo encoding is the following:

- Backlog_indicator: This flag indicates the presence of the Backlog field. Set to '1' to indicate the presence of backlog. Backlog is always present for inroute BARs or Ranging Requests, unless there is no backlog.

- Adaptation_indicator: This field indicates the presence/absence of the Adaptation field. Set to '0' to indicate that an Adaptation field is present.

- Version: This field identifies the version of the protocol. The use of version numbers allows future message changes. The specification for this document is version 1.

- Reserved: Set by the IPoS terminal as 0 and ignored by the hub on reception.

- Adaptation_Length: Indicates the number of bytes used by the Adaptation field if the Adaptation_indicator is set. A value of 0 indicates that the Adaptation_Length field is 2 bytes long; a value of 1 indicates that the Adaptation_Length field is 1 byte long.

- Serial_number: This field contains an IPoS terminal's 26-bit serial number.

- Backlog: This 2-byte field supports prioritized Backlog information. The first byte provides the total Backlog in bytes. It is encoded as a floating point number with a 2-bit exponent field and a 6-bit mantissa and shall be rounded out by the IPoS terminal. The Backlog shall be indicated by

$$8^{Backlog[7:6]} \times Backlog[5:0] \times 2.$$

This shall yield an even number up to 64K, which is the maximum practicable queue size to be tracked since this will fully occupy a 256 ksps inroute for 2 seconds. The two high-order bits in the second byte are set to '00', and the remainder of the byte identifies the percentage (of the Backlog that belongs to the priority indicated by the two higher-order bytes) in 1/64 units (the value is ((n+1)/64)*backlog where "n" is the number provided).

4.11.1.1.3 Adaptation Field

The Adaptation field serves two purposes:

1. The first is to provide management and control information along with the MAC header. Some examples of management and control information are remote configuration information or Ranging Request.

2. The second purpose is padding. The Adaptation field is adjusted to ensure that the MAC PDU fits the aggregated payloads of the group of bursts exactly.

The Adaptation field, when present, is defined by the first 2 bytes after the MAC header:

- The first byte indicates the total length of the Adaptation field in bytes

- The second byte is a bitmask defining which, if any, of the optional Adaptation fields described in the following subsections are present.

For Turbo code, if the MAC header for an unallocated channel's Adaptation_Length indicates that adaptation is 1-byte long, this Adaptation field will indicate the total length of the Adaptation field in bytes

Any remaining bytes indicated in the length byte that do not associate to one of the optional fields are stuffing bytes and will be set to 0.

The following subsections define the optional Adaptation fields that would be defined in the adaptation bitmask.

4.11.1.1.3.1 Reset Indication (Bit 7)

When bit 7 in the bitmask field of the Adaptation field is set to '1' by the IPoS terminal, the Reset Indication option is included in the Adaptation field. The Reset Indication option provides information about the IPoS terminal resetting of any compression history; the information elements and meaning in the Reset Indication option are given in table 4.11.1.1.3.1-1.

Table 4.11.1.1.3.1-1. Reset Indication Format

Field Name	Field Length (Bits)	Description
Terminal_version	32	This field provides the version number of the IPoS terminal embedded software.
DstIP	32	This shall be the IP address of the default hub that the IPoS terminal has been configured to use at commissioning time.

4.11.1.1.3.2 Ranging Request (Bit 6)

When bit 6 in the bitmask of the Adaptation field is set to '1' by the IPoS terminal, the Ranging Request option is included in the Adaptation field. The Ranging Request option shall be included in all ranging bursts; the information elements and meaning in the Ranging Request option are given in table 4.11.1.1.3.2-1

Table 4.11.1.1.3.2-1 Ranging Request Format

Field Name	Field Length (Bits)	Description
SQF	8	This field contains the current receive DEMOD SQF value.
Power_level	8	This field contains the PWM value used to control the transmit power level for this ranging burst.
Time_offset	8	This field is used to indicate the local timing offset (in the timing unit of 0.1 microsecond) that is being used to transmit the ranging packet. Values greater than 255 will be truncated.

4.11.1.1.3.3 Bandwidth Allocation Request

A remote terminal indicates to the hub that the unallocated Aloha transmission is a BAR packet by setting the Backlog_indicator to '0' and setting the Adaptation_indicator fields in the MAC header to '1'. Under these conditions, the terminal announces to the hub that there is a nonzero backoff request for bandwidth.

4.11.1.1.4 Payload

A remote terminal can send user information over the Payload field of inroute unallocated logical channels designated for Aloha transmission. The inroute user information, or IP datagrams, shall be segmented as defined in subsection 4.11.2. There is not a relationship between the datagram boundaries and the boundaries of the Payload field in the MAC format for unallocated inroute channels.

The number of bytes, N, in the payload field can be derived by subtracting the size of the other fields in the packet and the CRC-16 from the packet length configured for the Aloha logical channel. Depending on the configured length, the Payload field might contain a segment of an IP datagram or multiple IP datagrams.

4.11.1.1.5 Trailer Field

The CRC-16 is used over the Trailer field for the purpose of detecting errors occurring in the transmission of MAC PDU over the unallocated channels, both with convolutional and Turbo coding.

The CRC-16 is calculated with the following polynomial:

$$x^{16} + x^{15} + x^{2} + 1$$

The preset (initial) value is 0x0000.

The following steps describe the operation of the calculation of the CRC-16 by the IPoS terminal:

- Before CRC processing, each delay element is set to its initial value '0'.
- The switches are set in position A.
- The entire MAC PDU, with the exception of the CRC field, is shifted and simultaneously transmitted through the shifted datagram, starting from the IP source address field, passing through the shift register cells with the connections of the CRC-16 polynomial and simultaneously transmitted to the output.
- The content of the shift register after passing the last bit is the CRC-16, which is appended in the trailer field of the MAC PDU.
- The switches are moved to position B.
- The shift register is clocked 16 times, and the content of the shift register is transmitted to the output, starting with the bit at the end of the shift register.

Figure 4.11.1.1.4-1 shows a typical implementation of the logic used to calculate CRC-16.

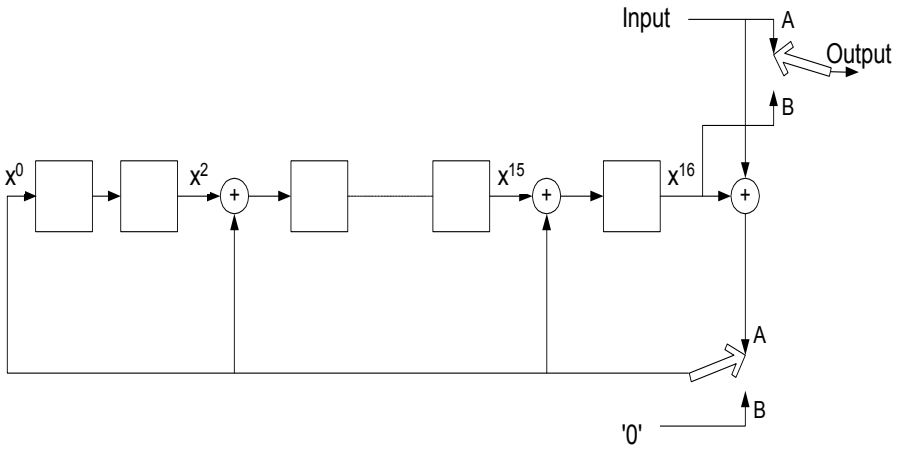


Figure 4.11.1.1.4-1. CRC-16 Calculation

At the hub, the CRC is computed in an identical manner on the received data. MAC PDUs with an invalid CRC-16 are dropped, but statistics of the CRC failures are retained by the hub.

4.11.1.2 MAC Formats for Allocated Channels

The MAC format used to encapsulate user information over allocated channels contains the same four-section structure of a MAC PDU for unallocated channels:

1. MAC header
2. Adaptation field
3. Payload or IP datagram fragment
4. Trailer field

The encapsulation of the datagram in the inroute MAC PDU for allocated channels is shown in table 4.11.1.2-1.

Table 4.11.1.2-1. Inroute MAC PDU Format

Field Name	Field Length (Bytes)	Comments
Header	5 or 8	5 bytes for Turbo coding 8 bytes for convolutional coding
Adaptation	0 to M	
Datagram bytes	N	
CRC-16	2	

The MAC header format for the allocated channels varies depending on whether the coding used in the PHY is convolutional or Turbo encoding. Also, the inroute MAC structure might include an Adaptation field that is used to convey management information to the hub and also is used for padding the MAC PDU to the combined payload of the group of inroute bursts.

4.11.1.2.1 MAC Header for Allocated Channels with Convolutional Coding

The MAC header for sending IP datagrams over the inroute allocated channels with convolutional coding is shown in table 4.11.1.2.1-1. The size of the MAC header for convolutional coding is 48 bits in the absence of the optional Backlog field, and 64 bits when the Backlog field is present.

Table 4.11.1.2.1-1. MAC Header for Allocated Channels with Convolutional Coding

Field Name	Field Length (Bits)
SeqNr_low	8
Backlog_indicator	1
Adaptation_indicator	1
Frame_number	2
BurstNr	4
Length_FEC	8
Length	8
SeqNr_high	8
Start_of_new_IPdatagram	1
Reserved	1
Traffic_priority	2
Reserved	4
Backlog	16

The description of the fields in the MAC header for allocated channels with convolutional coding is the following:

- SeqNr_low: This field contains the 8 LSBs of the Sequence Number field that are used for retransmission protocol. Note that the sequence number is for the priority whose datagram is at the beginning of the burst. The sequence number is split due to requirements at the hub on the location of the length field and on the first 13 bits being nonzero.

- Backlog_indicator: This flag indicates the presence of the Backlog field. Set to '1' to indicate the presence of Backlog.

- Adaptation_indicator: This field indicates the presence/absence of the Adaptation field. Set to '0' to indicate that the Adaptation field is present.

- Frame_number: This field contains the two LSBs of the frame number. This field helps the hub determine which burst was received.

- BurstNr: This field indicates the slot in the frame in which this burst was transmitted. With the addition of the inroute and frame number upon which it was received, the hub will be able to uniquely identify the source (SerNr and SrcIP) and destination (DstIP).

- Length_FEC: This field indicates the FEC value for the burst length.

- Length: This shall be the length of the burst. It includes all the bytes starting with the Backlog_indicator field through the CRC.

- SeqNr_high: This field contains the 8 MSBs of the Sequence Number field that are used for the retransmission protocol. Note that the sequence number is for the priority whose datagram is at the beginning of the burst. This is the selective acknowledgment, sliding window, byte

address of the first byte of the Encapsulated Datagrams field. With a 32 kbyte window size, this is large enough for 1 second at 256 ksps.

- Start_of_new_IPdatagram: This field indicates if the following datagram is the start of a new IP datagram or the continuation of a previous IP datagram. A value of 1 indicates that the start of a new IP datagram follows; a value of 0 indicates that a continued IP datagram follows.

- Reserved: The IPoS terminal sets this field to 0.

- Traffic_priority: This field indicates the priority level of the datagram at the beginning of the burst. Note that a preempted datagram may continue in the burst, and this continuing datagram may be at a different priority level than the datagram at the beginning of the burst. This field allows up to four priorities, with the value 0 indicating the highest priority.

- Reserved: This field is set to the value 0 and ignored by the hub.

- Backlog: This 2-byte field supports prioritized Backlog information. The first byte provides the total backlog in bytes. It is encoded as a floating point number with a 2-bit exponent field and a 6-bit mantissa and shall be rounded up by the IPoS terminal. The Backlog shall be indicated by

$$8^{\text{Backlog}[7:6]} \times \text{Backlog}[5:0] \times 2.$$

This shall yield an even number up to 64K, which is the maximum practicable queue size to be tracked since this will fully occupy a 256 ksps inroute for 2 seconds. The two high-order bits in the second byte are set to '00', and the remainder of the byte identifies the percentage (of the backlog that belongs to the priority indicated by the two higher-order bytes) in 1/64 units (the value is ((n+1)/64)*backlog where n is the number provided).

4.11.1.2.2 MAC Header for Allocated Channels with Turbo Coding

The MAC header for sending IP datagrams over the inroute allocated channels with Turbo coding is shown in table 4.11.1.2.2-1. The MAC header size for Turbo coding is 24 bits in the absence of the optional Backlog field, and up to 40 bits when the Backlog field is present.

Table 4.11.1.2.2-1. MAC Header for Allocated Channels with Turbo Coding

Field Name	Field Length (Bits)
Backlog_indicator	1
Adaptation_indicator	1
Start_of_new_IPdatagram	1
Reserved	1
Traffic_priority	2

Table 4.11.1.2.2-1. MAC Header for Allocated Channels with Turbo Coding

Field Name	Field Length (Bits)
Reserved	1
Adaptation_length	1
Sequence_number	16
Backlog	16

The description of the fields in the MAC header for allocated channels is the following:

- Backlog_indicator: This flag indicates the presence of the Backlog field. Set to '1' to indicate the presence of backlog.
- Adaptation_indicator: This field indicates the presence/absence of the Adaptation field. Set to '0' to indicate Adaptation field is present.
- Start_of_new_IPdatagram: This field indicates if the following datagram is the start of a new IP datagram or the continuation of a previous IP datagram. A value of 1 indicates that the start of a new IP datagram follows; a value of 0 indicates that a continued IP datagram follows.
- Reserved: The IPoS terminal sets this field to 0.
- Traffic_priority: This field indicates the priority level of the datagram at the beginning of the burst. Note that a preempted datagram may continue in the burst, and this continuing datagram may be at a different priority level than the datagram at the beginning of the burst. This field allows up to four priorities with the value 0 indicating the highest priority.
- Reserved: This field is set to the value 0 and ignored by the hub.
- Adaptation_length: This field indicates the number of bytes used for the length of the Adaptation field if the Adaptation field is present. The value '0' indicates that the number of bytes used for the length of the Adaptation field is 2 bytes. The value '1' indicates that the length of the Adaptation field is in a single byte.
- Sequence_number: This field is used for the retransmission protocol. This is the byte address of the first byte of the encapsulated payload or IP fragment.
- Backlog: This 2-byte field supports backlog information. The first byte provides the total Backlog in bytes. It is encoded as a floating point number with a 2-bit exponent field and a 6-bit mantissa and shall be rounded up by the IPoS terminal. The Backlog shall be indicated by

$$8^{\text{Backlog}[7:6]} \times \text{Backlog}[5:0] \times 2.$$

This shall yield an even number up to 64K, which is the maximum practicable queue size to be tracked since this will fully occupy a 256 ksps inroute for 2 seconds. The two high-order bits in the second byte are set to '00', and the remainder of the byte identifies the percentage (of the backlog that belongs to the priority indicated by the two higher-order bytes) in 1/64 units (the value is ((n+1)/64)*backlog where n is the number provided).

4.11.1.2.3 Adaptation Field

The Adaptation field for allocated channels serves the same purposes and includes the same options as does the Adaptation field for unallocated channels described in subsection 4.11.1.1.3. With Turbo coding, the number of bytes used to indicate the total length of the Adaptation field is determined by the Adaptation_length filed in the MAC header.

4.11.1.2.4 Trailer Field

The Trailer field for MAC PDUs over allocated channels is the CRC-16 described in subsection 4.11.1.1.4.

4.11.2 Inroute Segmentation

This subsection defines the segmentation that might take place in the inroute direction to divide higher level units of information, user IP packets, or control messages into one or more fragments that fit into the datagram_bytes section of the MAC PDUs. The mapping of IP packets into multiple MAC PDUs provided by inroute segmentation is intended to allow an efficient distribution of inroute capacity among the population of IPoS terminals.

To support the reassembling of all the fragments generated by the IPoS terminals at the hub, fragmentation delimiters are defined for the inroute direction. These delimiters shall be used on the inroute allocated channels depending on the following factors:

- Start of a new IP datagram for a given priority at the start of a burst. Also, the start of a new IP datagram for a given priority offset in the burst if the priority for the new IP datagram is the same as the priority for the IP datagram at the beginning of the burst.

- Start of a new IP datagram for a given priority offset in the burst. The new IP datagram that is starting offset in the burst is from a different priority than the IP datagram at the beginning of the burst.

- Continuation of an IP datagram for a given priority at the start of a burst.

- Continuation of an IP datagram for a given priority offset in the burst. The continuing IP datagram that is offset in the burst is from a different priority than the IP datagram at the beginning of the burst.

The appropriate fragmentation is part of the payload section of the MAC PDU and shall always be present before the start of the datagram. This presence is independent of whether the fragment is starting at the beginning of an IP datagram or offset in the IP datagram.

4.11.2.1 Start Fragmentation Header – Beginning of MAC PDU

The start fragmentation header described in this subsection shall be used when a new IP datagram for a given priority starts at the beginning of a MAC PDU or if a new IP datagram starts offset in the MAC PDU and the preceding datagram was from the same priority. For this start fragmentation header, the Start_of_new_IPDatagram field shall be set to '1'.

Table 4.11.2.1-1 shows the payload of the MAC PDU consisting of the start fragmentation header followed by the rest of the IP datagram fragment.

Table 4.11.2.1-1. Start Fragmentation Header – Beginning of MAC PDU

Field Name	Field Length (Bits)
Start_of_new_IPdatagram	1
Reserved	1
Traffic_priority	2
Datagram_counter/CRC	12
Protocol_version	4
Header_length	4
Type_of_service	8
Reserved	2
Reserved	3
Length	11
Rest_of_datagram	N×8

The description of the fields for the start fragmentation header for the new IP datagrams is:

- Start_of_new_IPdatagram: This field indicates if the following datagram is the start of a new IP datagram or the continuation of a previous IP datagram. A value of '1' indicates that the start of a new IP datagram follows; a value of '0' indicates that a continued IP datagram follows.

- Reserved: The IPoS terminal sets this field to 0.

- Traffic_priority: Used to allow up to four priorities, with the value 0 indicating the highest priority.

- Datagram_counter/CRC: This field shall be filled with the 12-bit CRC (CRC-12) described in subsection 4.11.2.5. The CRC-12 shall be calculated by the IPoS terminal before header compression.

- Protocol_version: This field takes the value 4 for IPv4.

- Header_length: This field in IP shall be the IP header length.
- Type_of_service: This field in IP shall be the type of service.
- Reserved: The IPoS terminal sets this field to 0.
- Reserved: The IPoS terminal sets this field to 0.
- Length: This field shall be used to indicate the length of the datagram, starting with the protocol version field. This field is 11 bits long because the maximum datagram is less than 2000 bytes on the IPoS system.
- Rest_of_datagram: The value of N is derived from the Length field.

4.11.2.2 Start Fragmentation Header – Offset in MAC PDU

The start fragmentation header described in this subsection shall be used when a new IP datagram for a given priority starts offset in a MAC PDU, and it is from a different priority than the preceding datagram. For this start fragmentation header, the Start_of_new_IPDatagram field shall be set to '1'.

Table 4.11.2.2-1 shows the payload of the MAC PDU consisting of the Start Fragmentation header followed by the rest of the IP datagram fragment.

Table 4.11.2.2-1. Start Fragmentation Header Offset – in MAC PDU

Field Name	Field Length (Bits)
Start_of_new_IPdatagram	1
Reserved	1
Traffic_priority	2
Datagram_counter/CRC	12
Sequence_number	16
Protocol_version	4
Header_length	4
Type_of_service	8
Reserved	2
Reserved	3
Length	11
Rest_of_datagram	N×8

The description of the fields for the start fragmentation header for the new IP datagrams is the following:

- Start_of_new_IPdatagram: This field indicates if the following datagram is the start of a new IP datagram or the continuation of a previous IP datagram. A value of 1 indicates that the start of a new IP datagram follows; a value of 0 indicates that a continued IP datagram follows.
- Reserved: The IPoS terminal sets this field to 0.

- Traffic_priority: Used to allow up to four priorities, with the value 0 indicating the highest priority.

- Datagram_counter/CRC: This field shall be filled with the 12-bit CRC (CRC-12) described in subsection 4.11.2.5. The CRC-12 shall be calculated by the IPoS remote before header compression. The Sequence Number field shall not be included in the CRC calculations.

- Sequence_number: This field shall contain the 16-bit sequence number for the given priority. The sequence number is used to support the retransmission protocol if the real-time traffic bit is not set. The inserted Sequence_number field shall not be considered part of the original stream, so the 2 bytes used by this field should not affect the "running" sequence number.

- Protocol _version: This field takes the value 4 for IPv4.

- Header_length: This field in IP shall be the IP header length.

- Type_of_service: This field in IP shall be the type of service.

- Reserved: The IPoS terminal sets this field to 0.

- Reserved: The IPoS terminal sets this field to 0.

- Length: This field shall be used to indicate the length of the datagram starting with the protocol version field. This field is 11 bits long because the maximum datagram is less than 2000 bytes on the IPoS system.

- Rest_of_datagram: The value of N is derived from the Length field.

4.11.2.3 Continuation Fragmentation Header – Beginning of MAC PDU

The continuation fragmentation header described in this subsection shall be used when an IP datagram for a given priority continues at the beginning of a MAC PDU. For this continuation fragmentation header, the Start_of_new_IPDatagram field header shall be set to '0'.

Table 4.11.2.3-1 shows the payload of the MAC PDU consisting of the continuation fragmentation header followed by the rest of the IP datagram fragment. Note that the Sequence_number field does not exist in this fragmentation header; the sequence number for the datagram is provided by the MAC header.

Table 4.11.2.3-1. Continuation Fragmentation Header – Beginning of MAC PDU

Field Name	Field Length (bits)
Start_of_new_IPdatagram	1
Reserved	1
Traffic_priority	2
Reserved	4
Rest_of_datagram	N×8

The description of the fields for the start fragmentation header for the new IP datagrams follows:

- Start_of_new_IPdatagram: This field indicates if the following datagram is the start of a new IP datagram or the continuation of a previous IP datagram. A value of 1 indicates that the start of a new IP datagram follows; a value of 0 indicates that a continued IP datagram follows.
- Reserved: The IPoS terminal sets this field to 0.
- Traffic_priority: Used to allow up to four priorities, with the value 0 indicating the highest priority.
- Reserved: This field is set to the value 0 and ignored by the hub.
- Rest_of_datagram: The value of N is derived from the Length field.

4.11.2.4 Continuation Fragmentation Header – Offset in MAC PDU

The continuation fragmentation header described in this subsection shall be used when an IP datagram for a given priority start continues at the offset in a MAC PDU. For this continuation fragmentation header, the Start_of_new_IPDatagram field in the MAC PDU header shall be set to '0'.

Table 4.11.2.4-1 shows the payload of the MAC PDU consisting of the continuation fragmentation header followed by the rest of the IP datagram fragment.

Table 4.11.2.4-1. Continuation Fragmentation Header – Offset in MAC PDU

Field Name	Field Length (bits)
Start_of_new_IPdatagram	1
Reserved	1
Traffic_priority	2
Reserved	4
Sequence_number	16
Rest_of_datagram	N×8

The description of the fields for the start fragmentation header for the new IP datagrams follows:

- Start_of_new_IPdatagram: This field indicates if the following datagram is the start of a new IP datagram or the continuation of a previous IP datagram. A value of 1 indicates that the start of a new IP datagram follows; a value of 0 indicates that a continued IP datagram follows.

- Reserved: The IPoS terminal sets this field to 0.

- Traffic_priority: Used to allow up to four priorities, with the value 0 indicating the highest priority.

- Reserved: This field is set to the value 0 and ignored by the hub.

- Sequence_number: This field shall contain the 16-bit sequence number for the given priority. The sequence number is used to support the retransmission protocol if the real-time traffic bit is not set. The inserted Sequence_number field shall not be considered part of the original stream, so the 2 bytes used by this field should not affect the "running" sequence number.

- Rest_of_datagram: The value of N is derived from the Length field.

4.11.2.5 Datagram CRC Calculation

This subsection details how to perform the CRC-12 calculation in the Datagram_counter/CRC field of the fragmentation header. The Datagram Counter/CRC field shall be filled in initially with a 12-bit datagram counter for non-real-time traffic and with zero for real-time traffic. The datagram counter is specific to each traffic priority and does not include real-time traffic within a priority.

The purpose of the Datagram_counter field is to detect loss of synchronization between the IPoS terminals and the hub. This ensures uncorrupted reassembly, correct destination addresses, correct decompressed packet length, and no loss of datagrams.

The CRC-12 is calculated with the following polynomial (0xF01):

$$x^{12} + x^{11} + x^{3} + x^{1} + 1$$

The preset (initial) value is 0xFFF.

The following steps describe the operation of the calculation of the CRC-12 by the IPoS terminal:

1. Before CRC processing, each delay element is set to its initial value '1'.

2. The datagram, starting from the IP Source Address field passes through the CRC with the initial vector set to the returned CRC value from step 1. The initial 12 bytes of the IP header are skipped over.

3. A trailer consisting of the IPoS terminal serial number (32 bits), Hybrid/IP Gateway IP address, and original IP length passes through the

CRC with the initial vector set to the returned CRC value from step 2 above.

4. After shifting the last bit of the trailer into the CRC-12, the output of all delay elements is read and the final CRC value is stored in the Datagram CRC field of the Datagram_counter/CRC field.

Failures on the CRC-12 shall be considered as synchronization failures. The hub shall force the IPoS terminal to the inactive state to initiate resynchronization. If the CRC-12 failure occurred on a datagram that was designated as real-time traffic, the resynchronization mechanism will not be employed, and the IPoS terminal will remain in the Active state.

4.12 MAC Procedures

4.12.1 System Timing

4.12.1.1 Overview

The IPoS system uses a star topology with the hub at the center of the star and the remote terminals at the points of the star. The hub sends a continuous DVB TDM (time division multiplexing) data stream to the satellite for broadcast to all the remote terminals in the coverage region. The remote terminals use TDMA to access shared inroute channels for transmissions through the satellite to the hub. TDMA requires that each remote terminal transmit its data bursts to the satellite for relay to the hub such that the bursts start within a narrow window of time, the aperture, within a specified burst of a particular frame at the hub. In the IPoS system, this aperture is 125 μs for assigned traffic bursts and Aloha bursts and 2 msec for ranging bursts (see subsection 3.5.4.1). The propagation time from a remote terminal to the hub through the satellite can vary by more than 10 msec from one remote terminal to another, depending on the position of the particular remote terminal on the Earth. This variation requires that each remote terminal execute procedures to determine exactly when it should transmit a data burst so that it will arrive at the hub within the proper 125 μs aperture.

Figure 4.12.1.1-1 shows the timing relationships between the hub and a remote terminal. A vertical line on the figure shows what is happening at the hub (at the top) and at the remote terminal (at the bottom) at the same time. The horizontal axis is marked in 45 msec units – the duration of an inroute frame. The hub is a constant reference for all IPoS system timing and frequency, and the remote terminals must establish an accurate time reference relative to the hub's fixed standard[3]. Note that:

$$T_{HO} = T_{H\text{-}S} + T_{S\text{-}R} + T_{RO} + T_{R\text{-}S} + T_{S\text{-}H}$$

[3] Note that this is different from a number of VSAT systems where the hub varies its time and/or frequency reference to compensate for satellite movement so that the timing at the remote terminals does not change.

where:

T_{HO}: hub offset time (time between transmission of $SFNP_N$ at the hub and the start of reception of frame N at the hub)

T_{H-S}: propagation time from hub to satellite (same value as T_{S-H})

T_{S-R}: propagation time from satellite to remote terminal (same value as T_{R-S})

T_{RO} remote terminal offset time (Time between "ideal" receipt of $SFNP_N$ at a remote and the transmit time for the start of transmission for frame N at this remote)

T_{R-S}: propagation time from remote terminal to satellite

T_{S-H}: propagation time from satellite to hub

$SFNP_N$: Superframe numbering packet that marks Frame N (Superframe number = N/8)

The hub-to-satellite round-trip time, $T_{H-S} + T_{S-H}$, can also be written as T_{H-S-H}.

Then:

$$T_{HO} = T_{H-S-H} + T_{S-R} + T_{RO} + T_{R-S}$$

If a remote transmits at the end of its T_{HO} interval, the hub will receive the burst in the first burst position within the frame. If the remote needs to transmit at some burst position later in the frame, it adds the time delay of this burst position to the end of the T_{HO} interval to give the time at which to transmit.

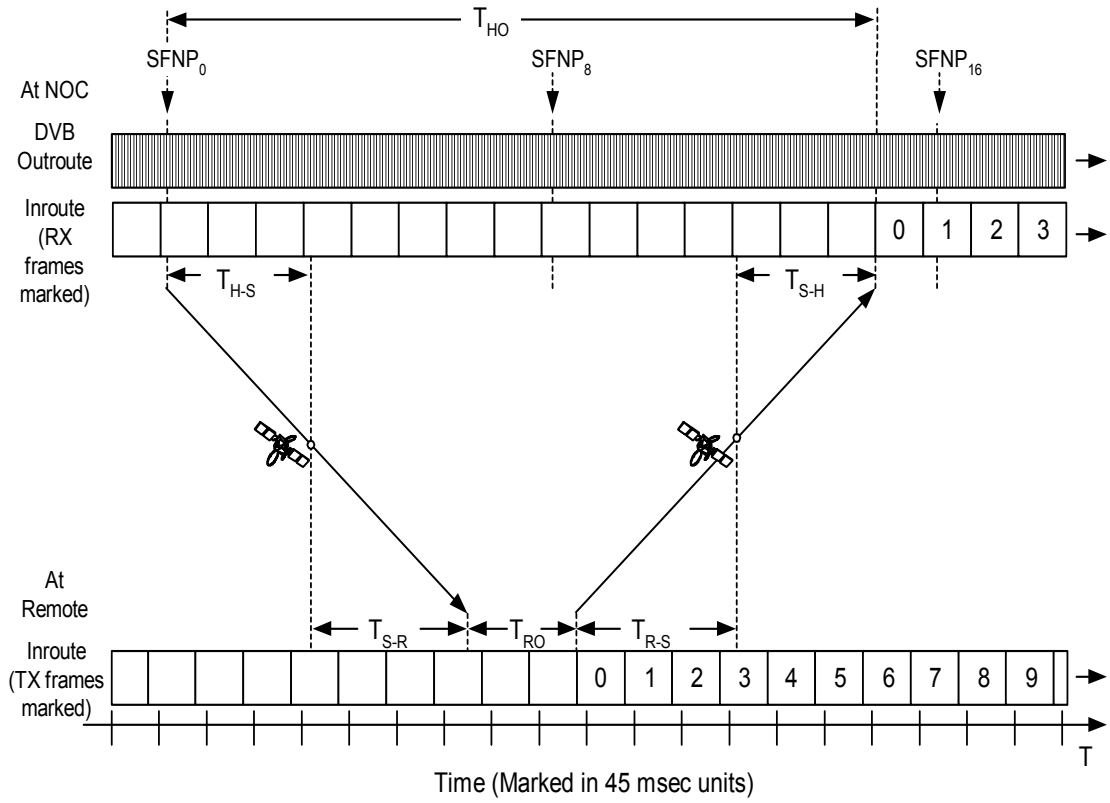


Figure 4.12.1.1-1. IPoS System Timing Relationships

By itself, the standard DVB outroute does not have any time marker that a remote terminal can use to synchronize its time reference with the hub's. However, the remote terminals must establish a time reference that is within 10s of μs of the hub's time reference so that they can transmit bursts that arrive at the hub in the assigned frames at the assigned times (i.e., within the right aperture). To provide this timing reference, the hub transmits an SFNP on the outroute once every superframe (eight frames, or 360 msec.). Table 4.13-4 in this section shows the format of the SFNP containing a frame number (not a superframe number), so the frame number in successive SFNPs increments by 8.

As Figure 4.12.1.1-1 shows, the hub starts the inroute TDMA frame one time interval specified in the Hub_timing_offset field in the SFNP message, T_{HO}, after it transmits the SFNP. Although the SFNP gives the value of T_{HO} in use, T_{HO} remains constant for a given system after it starts initial operation. T_{HO} must be set large enough that an SFNP can be received by a terminal that is farthest from the satellite, have that terminal do some processing (say two frames worth), then transmit a data burst in time to be received back at the hub at the start of the frame number given in the SFNP packet. A typical value for T_{HO} is 675 msec.

When a remote terminal has established its timing reference, T_{RO}, by ranging (see subsection 4.12.2), it will have determined its value for T_{RO} well within ± 62.5 μs of its exact current value. This allows the remote terminal to transmit a burst at the right time to fall within a 125 μs aperture at the hub.

Each of the following subsections describes specific procedures related to establishing and maintaining the proper value of T_{RO} at a remote terminal.

4.12.1.2 Variation in SFNP Transmission Time

The hub has a time reference, accurate to 1 part in 10^7, which allows the hub to determine when each new superframe (eight frames or 360 msec) starts. The hub tries to transmit the SFNP at exactly the start of every superframe. However, because of processing delays in the hub and because the DVB outroute transport packets are not synchronized with the hub's frame timing, the hub cannot transmit the SFNP at exactly the right time. The SFNP is always transmitted a little bit later than the "ideal," exact, 360 msec tick time. In addition, the amount of time that the SFNP is delayed from the ideal time varies slightly with each SFNP transmission.

Figure 4.12.1.2-1 shows an example of the ideal transmissions, the dotted lines, and the actual transmissions, the solid lines (with the delay from the ideal exaggerated). Although the delay and delay variation are small compared to the 360 msec superframe time, they are large compared to the accuracy that the remote terminals need to synchronize their timing with the hub's.

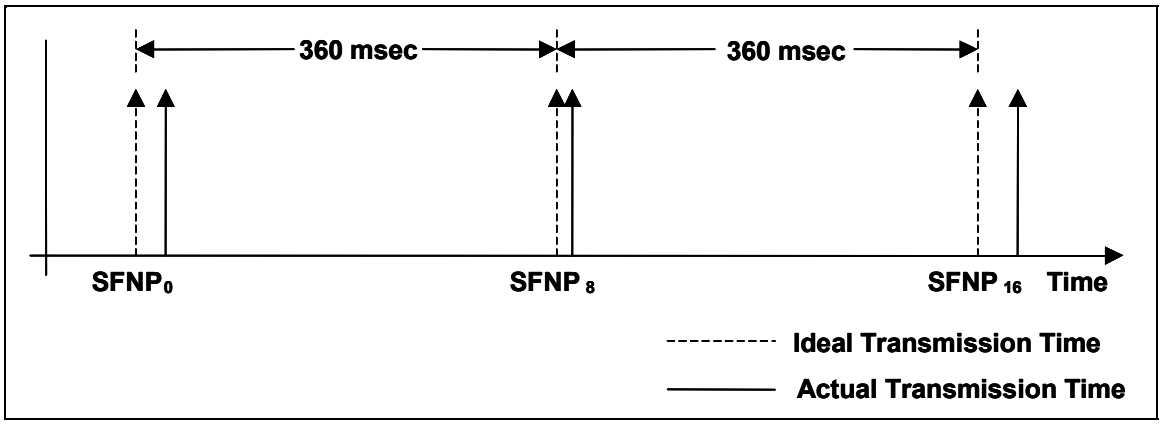


Figure 4.12.1.2-1. "Ideal" and Actual SFNP Transmission Time at the Hub

To allow remote terminals to correct for this variation, which occurs each time the hub transmits an SFNP, there is equipment at the hub measuring the time delay between the "ideal" exact time when the SFNP should have been transmitted (the start of the superframe) and the time when it was actually transmitted. The measured delay is provided by the hub to the remote terminals in the SFNP. Then the next SFNP gives the time that the previous SFNP was delayed from its "ideal" transmission time in the packet's Local SFNP Delay field. The remote terminals subtract this value from the time at which they received the previous SFNP to determine when it would have been received if the hub could have sent it at exactly the right time. This is the reference point that a remote terminal uses for its inroute frame timing calculations.

4.12.1.3 Timing Variation between Hub and Remote Terminal

The hub has a very accurate frequency/timing source (see subsection 3.3.6) that provides the SFNPs after corrections (see subsection 4.12.1.2) at 360 msec intervals with a high accuracy.

By contrast, the frequency/timing source at the remote terminal is less accurate and requires calibration. In IPoS the calibration of the remote terminal frequency/timing source is provided by the hub's frequency timing reference by comparing the time interval between received SFNPs with the elapsed time interval measured at the remote terminal local timing.

Remote terminals shall determine the corrections needed to their local reference by measuring a scaling factor that is the ratio of the interval between SFNPs, as received by the remote terminal, to 360 msec generated with the local timing of the remote terminal. Multiplying the local timer by the scaling factor remote terminals corrects the timing variations in their timing sources.

The remote terminals shall be constantly recalculating the time scaling factor to remove the drift in their local frequency/timing reference.

4.12.1.4 Superframe Synchronization

The hub transmits an SFNP once every superframe for each timing stream. A remote terminal processes each timing stream independently, as follows:

- The remote has synchronized to a stream if, having started unsynchronized, both of the following conditions are true:
  - Three consecutive valid SFNPs have been received.
  - After receiving consecutive valid SFNPs, the local timing matches within eight clock ticks.

Once a remote terminal has synchronized to a stream, synchronization is defined "to be lost" if any of the following conditions is true:

- Two consecutive SFNPs have been received with the local timing off by more than 16 clock ticks.
- No valid SFNP is received for three consecutive superframes.
- Two consecutive valid SFNPs have not been received for five superframe times.
- Three consecutive valid SFNPs have not been received for seven superframe times.

Annex A shows these conditions in a state diagram format.

4.12.1.5 Compensation for Satellite Distance Variations

Although the IPoS system uses a geosynchronous satellite, the position of the satellite is not perfectly fixed, as seen from a point on the earth. Because the satellite cannot be kept in a perfect orbit, the satellite moves slightly in azimuth and elevation as well as distance, as seen from both the hub and the remote terminals. This satellite movement changes the round-trip time between the hub and the remote terminals (i.e., the values of $T_{H\text{-}S\text{-}H}$, $T_{S\text{-}R}$, and $T_{R\text{-}S}$ defined in subsection 4.12.1.1). If there were no compensation for satellite movement, when the round-trip time from the hub to a particular remote decreased, the remote would receive its SFNPs earlier, and thus transmit its bursts to the hub earlier, relative to the frame timing at the hub. Furthermore, the hub would receive the bursts from the remotes earlier, relative to the frame timing at the remote, because of the reduced return distance from the remote to the hub. These effects would cause the hub to receive the remote's bursts earlier in the frame than before – possibly before the start of the receive aperture at the hub. Conversely, if the round-trip distance from the hub to a remote were to increase, the hub would receive that remote's bursts later, possibly after the end of the receive aperture. Therefore, the IPoS system has a mechanism for adjusting the transmit timing at the remote terminals to compensate for changes in round-trip time from the hub to the remotes.

It is not practical to measure the changes in the hub-to-remote round-trip times for *every* remote separately. Fortunately, the primary change in satellite position that affects round-trip times is movement closer to, or farther from, the Earth. As a first order approximation, this distance change is the same for the hub as for all of the remotes. The distance change is actually slightly different for each remote terminal and for the hub, but compensating for the "common mode" distance change is sufficient to allow all the remote terminal bursts to fall within the hub's receive apertures for the geosynchronous satellite required by the IPoS system (see subsection 2.2.1).

To determine the change in the distance (or actually, propagation time) from the hub to the satellite and back, the hub constantly measures the round-trip time through the satellite between itself and a collocated remote terminal and sends this measured time to the remotes in the SFNP. The current hub-to-satellite-to-hub time, $T_{H\text{-}S\text{-}H}$, is the Echo SFNP Delay field from the current SFNP minus the Local SFNP Delay field from the previous SFNP. A remote terminal can calculate the change in $T_{H\text{-}S\text{-}H}$ since it last ranged by subtracting the current $T_{H\text{-}S\text{-}H}$ value from $T_{H\text{-}S\text{-}H}$ at the time ranging was last completed. From subsection 4.12.1.1, a remote terminal's remote offset time, T_{RO}, is:

$$T_{RO} = T_{HO} - T_{H\text{-}S\text{-}H} - (T_{S\text{-}R} + T_{R\text{-}S})$$

The change in T_{RO} caused by the change in distance to the satellite is:

$$\Delta T_{RO} = - \Delta T_{H\text{-}S\text{-}H} - \Delta(T_{S\text{-}R} + T_{R\text{-}S})$$

T_{HO} is a constant, so it does not change. Since it is assumed that the change in hub-to-satellite-to-hub time, $\Delta T_{H\text{-}S\text{-}H}$, is, to a good approximation, the same as the change in the remote-to-satellite-to-remote time, $T_{S\text{-}R} + T_{R\text{-}S}$, then this equation can be rewritten as:

$$\Delta T_{RO} = -\ 2\Delta T_{H\text{-}S\text{-}H}$$

Thus, a remote terminal should constantly modify the value that it determined for the remote offset time, T_{RO}, the last time it ranged, by twice the change in $T_{H\text{-}S\text{-}H}$ from the last time it ranged. For example, suppose that when the remote terminal last ranged, the $T_{H\text{-}S\text{-}H}$ was 258,317 μs and the value of T_{RO} (determined accurately by ranging) was 98,921 μs. Then suppose that, at some later time, an SFNP packet shows that $T_{H\text{-}S\text{-}H}$ has changed to 258,307 μs. Then the remote terminal should set the T_{RO} value that it is using to 98,941 μs. That is:

$$\Delta\ T_{H\text{-}S\text{-}H} = -\ 10\ \mu s, \text{ or } \Delta T_{RO} = -\ 2\Delta T_{H\text{-}S\text{-}H} = +20\ \mu s$$

So, the remote terminal should *increase* its T_{RO} value by 20 μs to 98,941 μs. That is, the remote terminal should transmit its bursts 20 μs *later* relative to the receipt of the "ideal" SFNP than it did when it last ranged. It makes sense that if $T_{H\text{-}S\text{-}H}$ decreases by 10 μs, the remote should send its bursts 20 μs later than before. This is effectively increasing the total hub-to-remote-to-hub time so that the total remains the same. The change in $T_{H\text{-}S\text{-}H}$ is multiplied by 2 because there is also a remote-to-satellite-to-remote path in the hub-to-remote round-trip path, and its time has changed by about the same amount as $T_{H\text{-}S\text{-}H}$.

4.12.1.6 Resuming Operation After Interruption

It is necessary for an IPoS remote terminal to restart operation after an indefinite interruption without having to range again as long as the site and satellite locations have not changed. That means that the remote has to have a way to determine the current value of T_{RO} that it should use to time its transmissions based on the current distance to the satellite. Since remote terminals store the values of T_{RO} and $T_{H\text{-}S\text{-}H}$ in nonvolatile memory when they last ranged, they can calculate their current values for T_{RO} using the stored values and the current $T_{H\text{-}S\text{-}H}$ value contained in the latest SFNPs. The formula for calculating the current value of T_{RO} is:

$$T_{RO\ (current)} = T_{RO\ (at\ last\ ranging)} - 2\ (T_{H\text{-}S\text{-}H\ (at\ last\ ranging)} - T_{H\text{-}S\text{-}H\ (current)})$$

After reinitializing the value of T_{RO} according to the previous calculation, the remote terminals should resume the T_{RO} updating process described in subsection 4.12.1.5.

4.12.1.7 Timing Redundancy

The system timing function is critical to the operation of the IPoS. Therefore the IPoS standard contains an option for the hub to use redundant timing facilities to generate two independent timing "streams." When this option is implemented, the hub sends two SFNPs every superframe, one for each superframe timing stream. The SFNPs are marked with the ID of the timing stream, 0 or 1. Each remote processes the two timing streams independently with regard to superframe synchronization (see Annex A). If the terminal is in synchronization with either of the streams, the terminal is declared to be in superframe synchronization, and the terminal uses that stream for its timing calculations. If

the terminal loses synchronization on the online stream but maintains superframe synchronization on the other stream, it switches its timing calculations to the alternate stream. If the remote terminal is out of superframe synchronization on both timing streams, then the terminal is deemed to be out of superframe synchronization.

4.12.2 Remote Terminal Ranging

4.12.2.1 Purpose

The ranging process accomplishes the following:

- Determines accurately the remote offset time, T_{RO} (see figure 4.12.1.1-1), that the remote terminal should use to time its inroute transmissions.
- Enables a remote terminal to determine what types of available inroutes (transmission rates and coding methods) it is capable of operating within its current location and configuration.
- Determines the transmit power setting that the remote terminal should use for each type of inroute that is available and with which it is capable of operating.

A remote terminal executes the ranging process the first time that it operates at a particular site with a particular satellite, and each time a new inroute group type (transmission rate and coding) is made available to it.

4.12.2.2 Preparation for Ranging

Before a remote terminal begins the ranging process, it must:

1. Acquire the outroute using the configured outroute frequency and symbol rate (see subsection 3.8.1.1).
2. Synchronize its transmit frequency reference with the satellite outroute frequency so that it can transmit on inroutes with the required frequency accuracy.
3. Wait for superframe synchronization (see Annex A).
4. Wait for three additional superframe times after achieving superframe synchronization to be sure that it has received and stored a full cycle of IGDPs.
5. Estimate the distance from its location to the satellite using the configured values for site latitude and longitude and satellite longitude (see subsection 4.14). The remote terminal converts this distance to propagation time, $T_{S\text{-}R}$ (which is the same as $T_{R\text{-}S}$).

6. Estimate the value of T_{RO} using the formula given in subsection 4.12.1.1:

$$T_{HO} = T_{H\text{-}S\text{-}H} + T_{S\text{-}R} + T_{RO} + T_{R\text{-}S.}$$

7. This formula can be rearranged to:

$$T_{RO} = T_{HO} - T_{H\text{-}S\text{-}H} - (T_{S\text{-}R} + T_{R\text{-}S}).$$

8. Since $T_{S\text{-}R} = T_{R\text{-}S}$, This can also be written as:

$$T_{RO} = T_{HO} - T_{H\text{-}S\text{-}H} - 2T_{S\text{-}R}.$$

The values for T_{HO} and $T_{H\text{-}S\text{-}H}$ are known from the superframe numbering packets, and $T_{S\text{-}R}$ was estimated in step 5, above. The remote terminal cannot determine $T_{S\text{-}R}$ exactly since it does not know its own site location and the satellite location exactly. Therefore this is a first estimate for T_{RO}. The ranging process will help the remote terminal to determine the value of T_{RO} more precisely.

4.12.2.3 Ranging Order

Remote terminals typically receive multiple IGDPs describing different inroute groups. All of the inroutes in a particular group have the same transmission rate and coding method (64 ksps, 128 ksps, or 256 ksps with convolutional coding or 128 ksps or 256 ksps with Turbo coding). There may be multiple inroute groups that have the same transmission rate and coding method. The remote terminal performs the ranging process (see subsection 4.12.2.4) on one inroute group of each different inroute type in the following order:

1. 64 ksps, convolutional coding
2. 128 ksps, Turbo coding
3. 128 ksps, convolutional coding
4. 256 ksps, Turbo coding
5. 256 ksps, convolutional coding

The remote terminal skips the ranging process for any type that is not available (i.e., no IGDP was received for an inroute of that type), or if the terminal is not capable of transmitting on that type of inroute. For example, if a particular type of terminal were not capable of transmitting using convolutional coding, it would skip inroute groups of types 1, 3, and 5 above. The remote terminal terminates the ranging process when any of the following occurs:

1. The ranging process on this group type fails (see subsection 4.12.2.5).
2. The Ranging Acknowledgment command received at the end of the ranging process for a particular inroute has a Received E_b/N_0 field whose value is less than the E_b/N_0 Switchup field in the IGDP for this inroute group.

3. The ranging process was attempted on the last group of inroute types above, number 5.

4.12.2.4 Ranging Process

This subsection describes the steps that a remote terminal and the hub use to range on an inroute group of a specified type, transmission rate, and coding method.

The steps are:

1. The remote terminal:

    1.1. Selects an inroute group of the desired type, if there is more than one group of that type.

    1.2. Randomly selects an unallocated ranging logical channel from those whose location (frequency and burst position within a frame) are described in IGDPs.

    1.3. Transmits an inroute unallocated packet with a Ranging Request message at a default starting power level in the selected unallocated ranging logical channel. The transmission time is based on the initial estimate for T_{RO} (see subsection 4.12.2.2).

    1.4. Responds to ranging BAPs received from the hub by sending null data bursts or outstanding data, if any, in the assigned locations. If the remote terminal receives no response to its Ranging Request, it increases its power slightly and goes back to Step 1.1.

2. The hub:

    2.1. Receives the Ranging Request message from the remote.

    2.2. Sends a series of BAPs to the remote specifying an inroute, frame number, burst location, and burst length of the ranging burst that the remote should send. The remote responds to each allocation by sending a single ranging burst with the prescribed characteristics.

    2.3. Receives each ranging burst that the remote terminal sends and measures the time between the start of the aperture at the hub and the receipt of the packet from the remote. This aperture is about 2 msec long (compared to the 125 μs aperture that the hub uses for assigned data bursts and Aloha bursts from remote terminals that have already ranged).

    2.4. Stops sending BAPs to the remote and waits for the last ranging burst to be received.

    2.5. Averages the times between the start of the aperture and the receipt of the ranging burst for each ranging burst that the remote sent.

2.6. Sends this average time to the remote, in units of 0.1 μs, in the Timing Adjustment field of the Ranging Acknowledgment command portion of an ICAP.

3. The remote terminal receives the Ranging Acknowledgment command packet from the hub and increases or decreases its original estimate of T_{RO} so that the Timing Adjustment field would be a predetermined fixed value if the remote were to transmit another ranging burst. This predetermined value is a function of the inroute transmission rate and coding method. So, for example, if the predetermined value should be 500 μs, and the Timing Adjustment field value is 12,345 (or 1,234.5 μs, since the time is specified in 0.1 μs units), then the remote terminal should decrease its value for T_{RO} by 734.5 μs (1,234.5 μs–500 μs) so that its bursts will arrive at the hub 500 μs after the start of the receive aperture or 734.5 μs earlier than originally estimated.

4. The remote terminal stores the current values of T_{RO} and the round-trip time from the hub to the satellite, $T_{H\text{-}S\text{-}N}$, in nonvolatile memory. The remote terminal needs these values to compensate for changes in distance to the satellite and to resume operation after an interruption (see subsections 4.12.1.5 and 4.12.1.6).

5. The remote terminal adjusts transmit power such that the Received_E_b/N_o figure contained within the Ranging Acknowledgment command is equal to the E_b/N_o target field contained within the IGDP associated with the inroute group to which the IPoS remote is ranging.

Figure 4.12.2.4-1 shows the message sequence used in the remote terminal ranging process as described above. The remote terminal uses the information in the IGDP to select an unallocated ranging slot. The remote terminal then sends a Ranging Request packet in this slot. If the request is successful, the hub sends a series of BAPs; the remote terminal transmits a null burst in each of the assigned slots. When the hub has determined the timing correction and power adjustment that the remote terminal should use, it sends this information to the remote terminal in a Ranging Ack command.

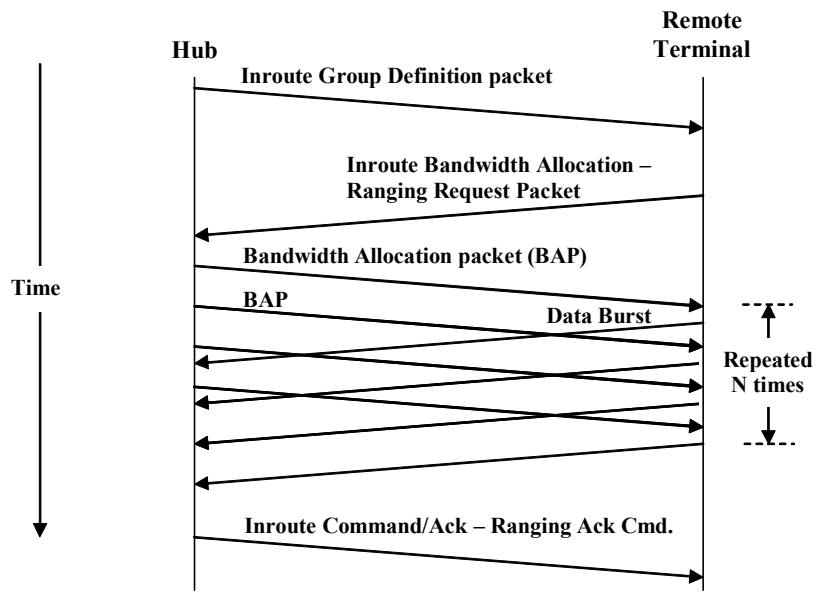


Figure 4.12.2.4-1 Message Sequence for Remote Terminal Ranging

4.12.2.5 Failure Conditions

There are four failure conditions that a remote terminal can encounter when attempting to range on a particular inroute type:

1. There are no unallocated ranging logical channels defined in any of the inroute groups of the desired type.

2. The remote terminal continues to retransmit Ranging Requests at higher and higher power until it has received no response at its maximum power.

3. The remote terminal stops receiving bandwidth allocations after making a Ranging Request but receives no Ranging Acknowledgment command after a timeout period.

4. The Received E_b/N_0 field in the Ranging Acknowledgment command received from the hub is below the E_b/N_0_min field in the IGDP for this inroute group.

If ranging fails, the remote terminal ends the overall ranging process described in subsection 4.12.2.4. If ranging has not been successful on any of the available inroute types, the terminal waits for a timeout period and then retries the overall ranging process from the beginning.

4.12.3 Inroute Group Selection by IPoS Remotes

The ranging process allows a remote terminal to determine the transmission rates and coding of available inroute groups. The remote terminal then picks the

"best" inroute type to use by picking the first available inroute type in the following order:

- 256 ksps Turbo coding
- 128 ksps Turbo coding
- 256 ksps convolutional coding
- 128 ksps convolutional coding
- 64 ksps convolutional coding

4.12.4 Inroute Data Transmission Sequence

4.12.4.1 Overview

As subsection 4.4.3 describes, the IPoS system does not use the concept of a user access session. Once a remote terminal has completed the start-up procedure (see subsection 4.4.2), it is always ready to transmit or receive data. An operational terminal can receive IP packets from an outroute at any time. It can also receive packets to be transmitted on the inroute at any time, but if it is idle (i.e., has not transmitted data on the inroute for some period of time), it must follow procedures for becoming active, sending data, and then returning to the Idle state. The following subsections describe these procedures.

4.12.4.2 Bandwidth Request and Acknowledgment

4.12.4.2.1 Aloha Logical Channel Selection

If a remote terminal has just started operation or if it has transmitted data and returned to the Idle state, it must request a bandwidth assignment from the hub before it can transmit data on the inroute. To do this, it follows these steps:

1. Selects an inroute group that contains one or more logical channels for Aloha bursts.
2. Randomly selects *two* specific Aloha logical channels (defined by their carrier frequency and timeslots) on which to transmit an Aloha BAR. These logical channels may be on the same inroute channel or they may be on different channels, but they must be sufficiently separated in time to allow the remote terminal to retune the inroute transmit frequency and transmit two bursts.

4.12.4.2.2 Aloha Request Transmission

Once the IPoS terminal has selected two Aloha logical channels on which to transmit its bandwidth request, it sends the *same* BAR in the two logical channels. The only difference in the contents of the two bursts is the fields that

indicate the frame and slot numbers in which the burst was transmitted and the CRC. Sending the bandwidth request twice is called Diversity Aloha. This technique decreases the likelihood that *both* requests will collide with other Aloha requests while keeping approximately the same Aloha channel throughput as a single-transmission logical Aloha channel.

The following fields are of particular importance in the Aloha requests:

- Remote Serial Number: This is how the hub identifies the remote terminal and how it determines the unicast MAC address used in data packets sent to this terminal.

- Backlog: This tells the hub how much data the remote terminal has remaining to be sent. This helps the hub allocate inroute bandwidth to terminals in proportion to the amount of data that they have to send.

- Encapsulated Datagrams: The terminal can send the first segment of the data that it has to send within the Aloha request itself. If the Aloha logical channels are configured to be large enough, the remote terminal may be able to send a complete transaction within the Aloha burst, depending on the application.

- Reset Indication: This Adaptation field gives the hub the remote terminal's IP address and the IP address of the IP packet processor within the hub, which should receive the packets from this remote. This second address is set in the terminal's Initial Configuration parameters (see subsection 4.14).

4.12.4.2.3 Bandwidth Request Acknowledgment

If the hub receives either of the remote terminals' two Aloha requests, it sends a single ICAP acknowledging receipt of one of the Aloha packets. The Aloha Acknowledgment command can acknowledge receipt of Aloha packets from a number of terminals in a single packet. Then, each remote terminal has to search each Aloha Acknowledgment command to see if its serial number is listed. If it is listed, the hub has received the Aloha request successfully.

If a remote terminal does not receive an ICAP acknowledging receipt of one its two Aloha transmissions within a timeout period, the terminal waits a random time (a random exponential backoff) and then transmits its Aloha request again.

4.12.4.3 Bandwidth Allocation

When the hub receives an Aloha bandwidth request from a remote terminal, it will begin sending the remote terminal BAPs, designating a frame number, starting slot number, and burst duration where the terminal may transmit. The hub sends BAPs for inroute frame N such that the remote terminal will always receive the BAP at least two frames before it needs to transmit data in response to the allocation arriving at the hub in frame N. The exact "lead time" between receipt of the BAP and the inroute frame being allocated depends on the value of

T_{HO}
(see subsection 4.12.1.1).

The hub typically sends one or more BAPs every frame time, 45 msec, allocating bandwidth for a particular frame, N, in the future. A BAP can assign bandwidth to more than one terminal that is using the same inroute group, so each remote terminal has to check each BAP to see if there is an allocation for an AssignID that matches the one that the terminal received when its Aloha bandwidth request was acknowledged.

The hub has to determine how to assign the inroute bandwidth based on the Aloha requests that it has received from remote terminals and the amount of data (shown in the Backlog field) that each remote terminal has to be sent. The hub generally assigns more bandwidth to terminals that have the highest backlog. However, the hub may give priority to remote terminals that have small amounts of data remaining since this data may be part of a short interactive transmission. If a terminal's backlog goes to zero, the hub does not immediately stop allocating bandwidth to the terminal. Depending on Configuration parameters, the hub may assign bursts at increasing intervals, say every other frame, then every fourth frame, etc., which allows the terminal to resume data transmission without having to send an Aloha burst. When the hub has not given a remote terminal a bandwidth assignment for a configurable number of frames, it moves the remote terminal's state to Idle and stops sending bandwidth assignments altogether until it receives another Aloha request from the terminal.

4.12.4.4 Inroute Data Transmission

A remote terminal must transmit a burst for each bandwidth allocation that it receives. If it has data to send, it sends as much of it as it can in the allocated burst. If it receives an allocation and has no data to send, it sends a null data packet. When the remote terminal is sending inroute data, it sends a Backlog field so that the hub will be able to judge how much bandwidth to allocate to this terminal.

A remote terminal sends the initial byte sequence number and the number of data bytes in each data burst that it sends. The byte sequence number starts at zero in the Aloha burst that requests bandwidth and in the next burst increases by the number of data bytes sent in the previous data burst. The byte sequence number field is 16 bits long and may roll over, if necessary. The hub sends an IAP for each inroute frame with a bitmap matching the corresponding BAP, indicating which bursts were received with correct CRCs. If a terminal receives an IAP indicating that its transmission for that burst was not received correctly at the hub, or if the remote does not receive an IAP within 16 frame times after it transmits a burst, it resends the data in the missed burst with the same byte sequence number as the one in the missed burst. Note that because the remote terminal receives varying burst assignments, it may be forced to send more bytes than were contained in the missed burst. The hub must detect the duplication and discard the duplicated bytes. When the remote resumes transmission, it continues from where it left off and transmits normally. This selective transmission scheme allows the invalid transmission to resume quickly and efficiently when the hub misses an inroute burst.

Note that the retransmission in acknowledged operation is on a burst-by-burst (or segment-by-segment) basis – not on an IP packet basis. The ensured delivery on the inroute operates below the level of the IP Packet Reassembly function.

4.12.4.5 Transition to Idle State

If a remote terminal does not receive a BAP with an assignment for its AssignID for a configurable number of consecutive frames, it transitions to the Idle state. This means that if the terminal currently has data to be transmitted or receives data in the future to be transmitted on the inroute, it will have to send another Aloha request as described above, starting with subsection 4.12.4.2.1, before it can resume sending data on the inroute.

While in the Idle state, the remote terminal prepares for the next ranging or Aloha access by obtaining the parameters every fourth frame in the superframe. These parameters will allow random-weighted selection among all the inroute groups advertised over the outroute. The selection of the inroute group involves the following initial steps:

1. Receive and process the IGDP messages.

2. Select the inroute groups that have transmission rates and coding methods supported by the terminal.

3. Eliminate any inroute groups that do not contain the type of unallocated channel, ranging or Aloha, required by the remote terminal. A value 0 in the Ranging_metric field indicates that the inroute group is unavailable for ranging; a value 0 in the bandwidth (Aloha)_metric indicates that the inroute group is not available for Aloha requests.

4.12.5 Contention Channel Access Procedures

Contention access procedures are used by the remote terminals to transmit over the inroute unallocated logical channels defined in subsection 4.11.1. These unallocated logical channels are made up of slots or group of slots within the inroute physical channels. The IGDP sent by the hub specifies the current locations (frequency and timeslots) of these unallocated channels. The unallocated channels are shared by multiple remote terminals on a contention basis, also designated as Slotted Aloha or random access.

Two types of structures are defined in IPoS for access on the inroute unallocated channels depending on whether the unallocated channels are designated for ranging or Aloha BARs. The communications procedure for accessing these two types of unallocated channels is the same contention access procedure described below despite the different burst lengths, apertures, and MAC formats that might be used for accessing these two types of unallocated channels.

When a remote terminal needs to transmit over an unallocated channel, it uses the following steps:

1. Performs a weighted selection based on the value of the metric field that pertains to the type of unallocated channel, Ranging_metric or Bandwidth (Aloha)_metric, to select an inroute group on which to transmit.

2. If a ranging channel is required, the remote terminal selects one of the defined ranging slots randomly. If an Aloha channel is required, the remote terminal selects two of the defined traffic slots randomly, with the constraint that the second slot does not overlap with the first in time and that the time separation between slots is sufficient to allow the terminal to change transmit frequencies, if required.

3. The terminal transmits the Ranging Request or BAR into the selected timeslot(s).

4. The remote terminal waits for the ICAP from the chosen group and for the inroute frame(s) in which the burst(s) were transmitted.

5. If the transmission was for ranging, the ICAP shows whether the hub received the Ranging Request. If the ICAP indicates that the hub has received the Ranging Request, the remote terminal proceeds to execute the ranging process as described in subsection 4.12.2.4. If the ICAP indicates that the hub did not receive the Ranging Request, the remote terminal goes back to step 1 after a time delay that is a random exponential delay whose parameters are contained within the IGDP.

6. If the burst is an Aloha BAR, the ICAP shows whether or not the hub has received either of the two Aloha transmissions. If the ICAP indicates that the hub has received any of them, the remote terminals proceed to execute the data transmission process as describe in subsection 4.12.4.4. If the IAP indicates that the hub did not receive either of the two Aloha bursts, the terminal goes back to Step 1 after a time delay that is a random exponential delay whose parameters are contained within the IGDP.

4.12.6 Packet Filtering Procedures

The IPoS outroute may contain a great deal of information that is not intended to be processed by a given remote terminal. To reduce the remote terminal's processing load, packet filters may be applied to the outroute to discard transport streams that are not intended for a particular remote terminal.

Packet filters are applied in the following order:

1. Filters to discard outroute packets that are not sent on transport streams associated with PSI tables and outroute logical control and traffic channels supported in the IPoS system as defined in subsection 4.9.2.

2. Filters to discard outroute packets that do not contain one of the following MAC addresses:

a) The remote terminal's unique unicast address (see subsection 4.10.1.3.1)

b) The multicast address to which the remote terminal might be configured to process multicast groups (see subsection 4.10.1.3.2)

c) The superframe numbering address (see subsection 4.10.1.3.3)

d) The return broadcast address (see subsection 4.10.1.3.4)

e) The return group address for the group with which the terminal is active (see subsection 4.10.1.3.5)

f) The unicast conditional access address unique to the remote terminal (see subsection 4.10.1.3.6)

g) The multicast conditional access address for the group with which the terminal is active (see subsection 4.10.1.3.7)

All other outroute packets shall be processed by the remote terminals to see if further processing is required.

4.13 Message Functional Definition and Contents

4.13.1 General

The requirements in this section are common to all exchanges of information over the IPoS air interface; they are intended to preserve the bit ordering, content, and length of the messages and their information elements.

The information received by the DLC from higher layers and transmitted to the PHY consists of sequences of bytes, or octets, with an integral number of bytes in the sequence.

4.13.2 Packet Order of Presentation

The order of presentation or transmission of both outroute and inroute IPoS packets by the remote terminals is in consecutive byte number, starting with byte 0 (header) and ending with the last byte, N. The remote terminal transmit order of presentation of the bits within each byte of a packet is MSB first (bit 7) and LSB last (bit 0). The packets are transmitted in order as shown by the direction of transmission in figure 4.13.2-1.

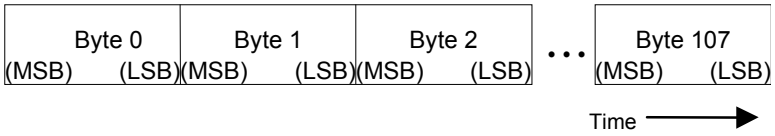


Figure 4.13.2-1. Packet Byte and Bit Order of Presentation

4.13.3 Order of Bits Within a Field

The order of bits within a field shall be "big-endian" as illustrated in figure 4.13.3-1.

(MSB) Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	(LSB) Bit 0	Byte
								N
				2^7	2^6	2^5	2^4	N+1
2^3	2^2	2^1	2^0					N+2
								N+3

Figure 4.13.3-1. Order of Bits Within a Field

Field values represented in hexadecimal (hex) notations that have four consecutive bits, or data nibble, are represented by a single character, X, from 0 to F (base 16). A 1-byte field value is represented by two nibbles as 0xXX, and a 2-byte value by four nibbles, with a leading zero in the form 0xXXXX. The hex representation of a 13-bit binary field might take values from 0x0000 to 0x1FFF.

Binary fields are represented by the corresponding string of zeros and ones with single quotation marks and the left-most bit, representing the MSB, e.g., '101001'.

Decimal values are presented in their natural format, e.g., 5.

4.13.4 Superframe Numbering Packet

SFNP contains measurements of the propagation time from the hub to the satellite and current propagation time in the hub. By using these times in combination with its own propagation time to the satellite, an IPoS terminal is able to calculate the time at which it should transmit a data packet such that it is received by the hub at the required time. Additionally, the SFNP identifies the IPoS network to which the IPoS terminal is connected.

The information elements in the SFNP are shown in table 4.13.4-1.

Table 4.13.4-1. SFNP Message Format

Field Name	Field Length (Bits)
Frame_type	8
Timing_source	1
Version	7
Frame_number	16
Local_SFNP_delay	32
Echo_SFNP_delay	32
SFNP_interval	32
Hub_timing_offset	32
Reserved	2
Frequency	15
Longitude	15
Reserved	1

Table 4.13.4-1. SFNP Message Format

Field Name	Field Length (Bits)
Reserved	1
Reserved	2
Ranging_identifier	4
Reserved	4
Modulator	4

The following is a description of the fields in the SFNP:

- Frame_type: Set to 0x01 by the hub, this field indicates an SFNP

- Timing_source: Set to '0' or '1' by the hub, it is used to distinguish the timing source at the hub (there are two for redundancy) generating this SFNP.

- Version: This field is set by the hub to indicate the return channel protocol version supported by the hub. This document describes version 1. If an IPoS terminal does not recognize a particular version of the message, it shall not transmit or use any of these incoming packets related to the return channels. Future versions of this protocol shall append only additional information onto this packet without changes to these existing fields. This action will permit the Beacon function for dish pointing to be maintained, regardless of version.

- Frame_number: This counter shall be incremented by eight by the hub for every superframe and shall be used to identify global timing. It will wrap every 49 minutes.

- Local_SFNP_delay: The value in this field is set by the hub to indicate the data propagation time at the hub. A value of 0 will be used to indicate that the value is unknown. IPoS terminals require two consecutive SFNPs to be able to interpret this field.

- Echo_SFNP_delay: The value in this field is set by the hub and used by IPoS terminals in the calculation of the round-trip delay from the hub to the satellite. The value of 0 will be used to indicate that the value is unknown for the previous superframe. IPoS terminals require two consecutive SFNPs to be able to interpret this field.

- SFNP_interval: The value in this field is set by the hub to indicate the elapsed time between this SFNP and the previous one. IPoS terminals shall use this information to adjust for any differences between their local measurement clock and the clock used by the timing units at the hub. The value of 0 shall be used to indicate to the IPoS remote that the value is unknown for the previous superframe. IPoS terminals are required to receive three consecutive SFNPs to be able to interpret this field.

- Hub_timing_offset: The value in this field is set by the hub to indicate the number of milliseconds between the IPoS outroute SFNP and the time that the first frame from the superframe will be received at the hub.

- Reserved: This field shall be transmitted by the IPoS hub as value '00' and confirmed by the IPoS remote upon reception. The 2 bits in this field, plus the Frequency and Longitude fields, are intended as a method of confirming that the correct satellite network is being monitored.

- Frequency: Set by the hub to the frequency of the outroute transponder. The frequency is measured in 100 kHz units.

- Longitude: Set by the hub to the longitude of the satellite. Bit 14 is the West/East_ indicator, bits 13 through 6 are the degrees, and bits 5 through 0 are the minutes.

- Reserved: Set to '0' by the hub.

- Reserved: Set to '0' by the hub.

- Reserved: Shall be transmitted by the hub as '00' and ignored upon reception at the IPoS terminals.

- Ranging_identifier: The value in this field is set by the hub and shall be stored by the IPoS remote when performing a ranging operation. If the received Ranging_identifier does not match the previously saved value, then the ranging information is invalid. The Ranging_identifier value is only changed to force all IPoS terminals to re-range to recover from some catastrophic error.

- Reserved: This field shall be transmitted by the IPoS hub as 0x0 and ignored by the IPoS remote upon reception.

- Modulator: This value shall indicate the type of modulator used for the outroute satellite transponder.

4.13.5 Inroute Group Definition Packet (IGDP)

IGDP messages are used to define the inroute logical on an inroute channel group and to determine which carriers of inroute channel groups are for user traffic and for request/ranging. Inroute channel groups are used to allow for load sharing among a number of inroute channels and to minimize the outroute bandwidth required to control the inroute channel bandwidth allocation. Inroute channel groups also limit the amount of information that needs to be cached or processed by the IPoS terminals.

All IPoS terminals on the same outroute carrier shall receive all IGDP messages sent on this outroute and ignore IGDP messages intended for other inroute groups. IPoS terminals shall discard the content of those messages that are not received again after three superframe intervals. The inroute group tables created

in the IPoS terminals from the information elements of all IGDP messages should be almost static, with the exception of the metrics.

The information elements in the IGDP message are given in table 4.13.5-1.

Table 4.13.5-1. IGDP Message Format

Field Name	Field Length (Bits)
Frame_type	8
Inroute_group_ID	7
Frequency_offset	5
Return_channel_type	4
Reserved	1
Reserved	2
Reserved	1
Reserved	4
Ranging_metric	8
Ranging_backoff	4
Ranging_retries	4
Ranging_max_backoff	16
Bandwidth (Aloha)_metric	16
Small_Aloha_backoff	4
Small_Aloha_retries	4
Reserved	4
Reserved	4
Aloha_max_backoff	16
E_b/N_o_switchup	8
E_b/N_o_target	8
E_b/N_o_min	8
Reserved	8
Frequency_table	N×24

The description of the fields in the IGDP is the following:

- Frame-type: Set to 2 to indicate an IGDP.

- Inroute_group_ID: This field is set by the hub to provide an identifier for each inroute group. This identifier shall be unique across all IPoS inroute groups that are available to a set of IPoS outroutes.

- Frequency_offset: Set to 7 by the hub for the version of the specification in this document. This field provides the offset into the packet (in 16-bit words) of the Frequency_table field from the start of the Aloha_max_backoff field. It shall be used to allow addition of future fields while maintaining backward compatibility.

- Return_channel_type: This field indicates the encoding and the transmitted symbol rate of the inroute channel. The MSB is set to '1' to indicate Turbo coding, and set to '0' for convolutional coding. The value of the lower 3 bits indicates the transmission rate according to the following settings:

Value	Standard Rate (ksps)
0	64
1	128
2	256
3	512
4	1024

- Reserved: Set to '0' by the hub.
- Reserved: Set to the value 0 by the hub. IPoS terminals shall ignore this field.
- Reserved: Set to '0' by the hub.
- Reserved: Set to the value 0 by the hub.
- Ranging_metric: This metric shall be used for a random-weighted selection of an inroute channel group when performing the nonallocated ranging procedure. It shall be based on the number of nonallocated ranging bursts defined and the collision rate on those bursts. A value of 0 in this field means that the nonallocated ranging procedure is not available on this inroute channel group.
- Ranging_backoff: The value in this field indicates the number of frames (minus one) for the initial random backoff for the ranging transmission.
- Ranging_retries: The value in this field indicates the number of times (minus one) that a packet retransmission shall be attempted using the initial random backoff before the IPoS terminal exits the ranging procedure.
- Ranging_max_backoff: After the ranging retries have been exceeded, the transmission is aborted, but the IPoS remote shall continue to attempt to recover in the background. This value is the upper limit for the truncated, binary exponential backoff algorithm that the IPoS remote shall use.
- Bandwidth (Aloha)_metric: This field is set by the hub and is intended to evenly distribute users between inroute groups. A value of zero indicates an unavailable inroute group or no Aloha operation defined for this group. This metric shall be used when the IPoS terminals become active for the random weighted selection of an inroute channel group. It shall be based on the ratio of the number of return channels available for user traffic to the active number of users.
- Small_Aloha_backoff: This field indicates the number of frames (minus one) for the initial random backoff for the small Aloha transmission.
- Small_Aloha_retries: This field shall indicate the number of times (minus one) that a packet retransmission is attempted using the initial random backoff before the IPoS terminal exits the Aloha procedure.

- Reserved: Set to 0 by the hub and ignored on reception.
- Reserved: Set to the value 0 by the hub.
- Aloha-max_backoff: This value is set by the hub to the upper limit for the truncated, binary exponential backoff algorithm.
- E_b/N_o_switchup: This field indicates the inroute E_b/N_o value required to attempt ranging up to the next available inroute symbol rate. Ranging to higher rates is done only if they are available. E_b/N_o values are indicated in 0.1 dB units.
- E_b/N_o _target: This field is set by the hub to indicate the desired (target) inroute E_b/N_o value for ranging on this inroute group. E_b/N_o values are indicated in 0.1 dB units.
- E_b/N_o_min: This field is set by the hub to indicate the minimum inroute E_b/N_o value required for ranging on this inroute group. E_b/N_o values are indicated in 0.1 dB units.
- Reserved: Set by the hub to the value 0 and ignored on reception.
- Frequency_table: This field indicates the frequency used to transmit on each of the inroute carriers in the group. There is an upper bound of no more than 4,000 inroute carriers within an inroute channel. The upper bound for the number of return channels in each return channel group is based on the limit of the number of burst allocations in the BAP since only a single BAP message is sent for each inroute group. If an inroute is not used, then its bandwidth will be allocated to a reserved AssignID from the BAP. The frequency is encoded as:

$$\text{Frequency} = 14\ \text{GHz} + \text{value} \times 100\ \text{Hz}$$

4.13.6 Inroute Command and Acknowledgment Packet (ICAP)

The ICAP message is used to convey an inroute acknowledgment that explicitly acknowledges Aloha and ranging transmissions over the unallocated inroute channels as well as sending commands to IPoS terminals. The ICAP messages are multicast to reduce outroute bandwidth.

The information elements in the ICAP are given in table 4.13.6-1.

Table 4.13.6-1. ICAP Message Format

Field Name	Field Length (Bits)
Frame_type	8
Number_of_entries	8
Offset_table	N×16
Command/Acknowledgment	M×8

The description of the fields and their values in the ICAP are as follows:

- Frame-type: Set to a value of 5 to indicate an ICAP
- Number_of_entries: The value in this field is the number of entries in the following Offset_table field.
- Offset_table: This is a table of offsets where each of the variable sized Command/Acknowledgment fields begins. The size should be known based on the Command field. Each offset is an 11-bit value and starts from the beginning of the Offset_table. The value of N is the number of entries. Note that since the offset is 11 bits, there are 5 reserved bits for each entry.
- Command/Acknowledgment: This is a list of commands or acknowledgments sorted by SerNr with the fields defined in the following subsections. No more than one command or acknowledgment can be sent to an IPoS terminal per packet.

The following subsections describe the commands that can be contained within an ICAP.

4.13.6.1 Ranging Acknowledgment Command

Table 4.13.6.1-1 gives the fields and description of the Ranging Acknowledgment command.

Table 4.13.6.1-1. Ranging Acknowledgment Command

Field Name	Field Length (Bits)	Description
SerNr	26	Set by the hub to the serial number of the IPoS remote in this field.
Command	5	A value of 0 shall indicate a Ranging (and Unallocated Ranging) Acknowledgment command from the IPoS hub. When an IPoS remote is using allocated ranging, it may not receive ranging acknowledgments for each frame, but the encapsulated datagrams will be acknowledged within the IAP. The hub shall transmit this acknowledgment upon the inroute group multicast address.
Reserved	1	Should be transmitted as 0 and ignored on reception.
Timing_adjustment	16	This is a signed 16-bit field indicating the number of μs by which to adjust the burst timing. The IPoS terminal shall alter its burst timing by the value commanded by this field.
Received_E_b/N_o	16	This is an unsigned 16-bit field that indicates the received E_b/N_o value at the hub at the previous ranging cycle.
Frame_number	16	This 16-bit field is the frame number to acknowledge.

4.13.6.2 Aloha Acknowledgment Command

Table 4.13.6.2-1 gives the fields and description of the Aloha Acknowledgment command.

Table 4.13.6.2-1. Aloha Acknowledgment Command

Field Name	Field Length (Bits)	Description
SerNr	26	The hub transmits the serial number of the IPoS terminal in this field.
Command	5	A value of 1 indicates an Aloha Acknowledgment. Only one of the diversity Aloha packets will be acknowledged. This acknowledgment is sent upon the inroute group's multicast address.
Reset	1	If this bit is set, it indicates that no prior state information on the IPoS terminal was maintained by the hub. This will cause the IPoS terminal to transmit its source and destination IP addresses.
Reserved	1	Should be transmitted as 0 and ignored on reception.
Inroute_group_ID	7	This is the inroute group, where future bandwidth will be allocated. The inroute type for this group must be the same type that was used in the Aloha packet.
AssignID	16	This is an ID used in BAPs. A value of 0 will acknowledge the data without assigning any bandwidth. If there was any backlog advertised from the Aloha packet, it will need to be flushed since the IPoS terminal remains inactive and no synchronization is possible.
Frame_number	16	This 16-bit field is the frame number to acknowledge.

4.13.6.3 Disable/Enable IPoS Terminal Command

Table 4.13.6.3-1 gives the fields and description of the Disable/Enable IPoS Terminal command.

Table 4.13.6.3-1. Disable/Enable IPoS Terminal Command

Field Name	Field Length (Bits)	Description
SerNr	26	The hub transmits the serial number of the IPoS terminal in this field.
Command	5	A value of 2 indicates a Disable/Enable IPoS Terminal Transmitter command – When disabled, the IPoS terminal will not transmit again until it is explicitly enabled from the hub. This setting is stored in nonvolatile memory on the IPoS terminal. There is no acknowledgment to this command.
Enable	1	Set to 1 if enable, set to 0 for disable.

4.13.6.4 Start Ranging Command

Table 4.13.6.4-1 gives the fields and description of the Start Ranging command.

Table 4.13.6.4-1. Start Ranging Command

Field Name	Field Length (Bits)	Description
SerNr	26	The hub transmits the serial number of the IPoS remote in this field.
Command	5	A value of 3 indicates a Start Ranging command. The IPoS terminal is informed that is required to range by having ranging bursts allocated. This command is implicitly acknowledged by the IPoS terminal ranging.
Invalidate	1	If this bit is set, the IPoS terminal will invalidate its prior ranging information and revert to the defaults.
Reserved	1	This field is set by the hub to '0' and shall be ignored by the IPoS remote.
Inroute_group_ID	7	This is the inroute group where the hub will allocate bandwidth to the IPoS terminal. This will imply the use of the associated inroute type when initiating ranging.
Reserved	16	This field is set by the hub to '0' and shall be ignored by the IPoS remote.

4.13.6.5 Go Active Command

Table 4.13.6.5-1 gives the fields and description of the Go Active command.

Table 4.13.6.5-1. Go Active Command

Field Name	Field Length (Bits)	Description
SerNr	26	The hub transmits the serial number of the IPoS terminal in this field.
Command	5	A value of 4 indicates a Go Active command. IPoS remotes will look for allocated bursts on the specified inroute group and transmit on the ones allocated to them. This command is only accepted if the IPoS remote is inactive and has already successfully ranged for the inroute type. This command is implicitly acknowledged by the act of transmitting.
Force_switch	1	If this bit is set, this will force a "special remote" to switch its inroute group.
Reserved	1	Should be transmitted as '0' and ignored on reception.
Inroute_group_ID	7	This is the inroute group where future bandwidth will be allocated.
AssignID	16	This is an ID used in the BAP.

4.13.6.6 Change Inroute Group Command

Table 4.13.6.6-1 gives the fields and description of the Change Inroute Group command.

Table 4.13.6.6-1. Change Inroute Group Command

Field Name	Field Length (Bits)	Description
SerNr	26	The hub transmits the serial number of the IPoS terminal in this field.
Command	5	A value of 5 indicates a Change Inroute Group command. This command is only accepted if the IPoS terminal is active. This command is implicitly acknowledged by the act of using the new inroute group.
Reserved	2	Should be transmitted as 0 and ignored upon reception.
Inroute_group ID	7	This is the ID of the inroute group where future bandwidth will be allocated. The inroute type for this group must be the same type that is currently in use.
AssignID	16	This is an ID used in the BAP. A value of 0 can be used to force an IPoS terminal inactive, but the preferred method is to remove its bandwidth allocation.

4.13.6.7 Reset Terminal Command

Table 4.13.6.7-1 gives the fields and description of the Reset Terminal command.

Table 4.13.6.7-1. Reset Terminal Command

Field Name	Field Length (Bits)	Description
SerNr	26	The hub transmits the serial number of the IPoS remote in this field.
Command	5	A value of 7 indicates a Reset Terminal command. This command forces the IPoS terminal to reboot within 10 seconds of receiving the command. This delay is included to debounce multiple copies of the command that may have been sent for redundancy. No attempt shall be made to shut down gracefully such as going inactive or informing the hub. There is no acknowledgment to this command.
Reserved	1	Should be transmitted as 0 and ignored upon reception.

4.13.7 Bandwidth Allocation Packet

IPoS terminals receive one BAP message each frame from the inroute group from which they are currently expecting to receive bandwidth. The IPoS terminal needs to scan the entire list in the Burst_allocation_record to derive the following elements needed in order to be able to transmit data and process acknowledgments:

- Inroute Group: Since the IPoS terminal can be monitoring two inroute groups it will need to confirm the inroute group based on the MAC address of the message and process only the BAP messages for which it expects to use bandwidth.

- Inroute Index: Computed as the cumulative Burst_offset divided by the slot size of a frame. It is used as an index into the Frequency_table of the Inroute Group Definition message.

- Frame Number: This element comes directly from the Frame_number field of the message.

- BurstId: This is the 4 LSBs of the index into the Burst_allocation_record.

- Burst Offset: The cumulative burst offset starts at 0 and increases with the each Burst_size. The burst offset is the cumulative burst offset modulo the slot size of a frame.

- Burst Size: This element comes directly from the Burst_allocation_record and will never cross a frame boundary.

- Acknowledgment Offset: This is the index into the entry's burst allocation table.

The format of the BAP message is given in table 4.13.7-1.

Table 4.13.7-1. BAP Message Format

Field Name	Field Length (bits)
Frame_type	8
Frame_number	16
Burst_allocation_record	24xN

The description of the fields and their values in the BAP is as follows:

- Frame-type: Set to 3 to indicate an BAP.

- Frame_number: This field indicates the Frame_number that is allocated in this message. The value of this field shall be larger than the current Frame_number; the difference is a fixed offset that allows the IPoS terminals to respond to changes in allocation.

- Burst_allocation_record: This is a list of all the burst allocations for each inroute. The format of each Burst_allocation_record is defined in table 4.13.7-2. The list contains all the bursts in a frame, and a frame for each inroute carrier in the group. The list is limited to no more than 489 entries, since IP datagrams are limited to 1500 bytes. It is important that the list of Burst_allocation_record is well ordered since the IPoS terminal performs a linear search. A malformed Burst_allocation_record can cause misoperation as there is limited error checking on this field.

Table 4.13.7-2. Format of the Burst_allocation_record

Field Name	Field Length (bits)	Description
AssignID	16	This is a unique identifier used to indicate to which IPoS terminal the bandwidth was allocated. The value of 0 is used to indicate small Aloha (and nonallocated ranging) bursts, and a value of 1 is used to indicate large Aloha bursts. The value of 0xFFFF will be used to indicate bandwidth that is not assigned.
Ranging	1	This indicates whether the burst is allocated for normal (value = '0') or ranging bursts (value = '1'). While an IPoS terminal is ranging it will still be able to send encapsulated datagrams over the inroute. An active user may have ranging turned on/off to test or fine tune the value with minimal impact on performance.

Table 4.13.7-2. Format of the Burst_allocation_record

Field Name	Field Length (bits)	Description
Final_burst	1	If the value is '1', this is the final burst that is being assigned to this remote for the current session.
Burst_size	6	Size (in slots) of this burst, including the aperture and burst overhead.

4.13.8 Inroute Acknowledgment Packet

The IAP message is used to explicitly acknowledge each inroute packet for assigned bandwidth with a good CRC, regardless of the presence of any encapsulation data. Besides allowing for faster recovery from inroute packet errors, this will also allow measurement of the inroute packet error rate at the IPoS remote. Aloha and nonallocated ranging packets are acknowledged explicitly.

If the IAP is lost, the IPoS terminal will retransmit the packet automatically except for any Constant Bit Rate (CBR) data that was in the lost burst. The loss of the IAP for a particular inroute group is detected when the next IAP packet is received or, if no IAP is received, for four frame times.

The information elements in the IAP message are given in table 4.13.8-1.

Table 4.13.8-1. IAP Message Format

Field Name	Field Length (bits)
Frame_type	8
Frame_number	16
ACK	N

The description of the fields and their values in the IAP is as follows:

- Frame_type: A value of 4 indicates an IAP.
- Frame_number: This field indicates the frame number for which the acknowledgment applies and must be less than the current frame number.
- ACK: This field is a bitmap that matches the entries for this frame in the burst allocation table of the BAP. To determine what was acknowledged, IPoS terminals must determine which bursts were assigned to them from the BAP and remember what data was transmitted during those bursts. The value of N is derived from the length of the IP datagram and will match the value of N from the associated BAP.

4.13.9 Periodic Adapter Conditional Access Update (PACAU)

The hub periodically transmits the PACAU packet containing the decryption element keys (EKs) used for the decryption of encrypted unicast traffic. The PACAUs also contain multicast group keys (GKs) for the multicast service elements for which the transceiver has been enabled. The PACAU can contain multiple GKs and EKs simultaneously, in which case the Group ID field will form an array of entries, one of which may be an EK. The PACAU is individually addressed to each IPoS remote's Unicast Conditional Access address.

For clarity, the PACAU packet has been split into two subsections. The first, the PACAU header, contains addressing and version information for the PACAU packet. The second, the PACAU array entry, contains the keys for each group or element of which the IPoS remote is a member, ordered by group ID. The PACAU header is defined in table 4.13.9-1, the PACAU payload for the GKs is given in table 4.13.9-2, and the PACAU payload for the EKs is defined in table 4.13.9-3.

Table 4.13.9-1. PACAU Header Format

Field Name	Field Length (Bits)	Description
PACAUVer	32	Current PACAU version for this IPoS terminal
ICAUVer	32	Current ICAU version for this IPoS terminal
Timestamp	64	ICAU_Request backoff time in seconds that the IPoS remote should randomize before sending an ICAU_Request
SiteID	80	This is the unique Site ID of the IPoS terminal provided to the IPoS remote in this packet.
EEMK	128	EEMK for this IPoS remote

Table 4.13.9-2. PACAU Group Key Entry Format

Field Name	Field Length (Bits)	Description
GroupID	24	Unique GroupID
Version	8	Current crypto version
Crypto Key	64	Crypto Key

Table 4.13.9-3. PACAU Element Key Entry Format

Field Name	Field Length (Bits)	Description
ElementID	24	Set to 0xFF
Version	8	Current crypto version
Crypto Key	64	Crypto Key

The PACAU EK payload is distinguished from the PACAU GK payload by the EK's payload Element ID field value being equal to 0xFF.

4.13.10 Interactive Conditional Access Update (ICAU) and Response (ICAU-R)

The ICAU command contains EKs used for the decryption of encrypted unicast traffic. The ICAUs also contain GKs for the multicast groups for which the remote terminal has been enabled. The ICAU is individually addressed to each IPoS remote's unicast conditional access address and is only made available to the IPoS remote by a telephone line. The ICAU is used principally as a part of terminal commissioning, where RF connectivity has yet to be established.

The current ICAUVer is broadcast in the PACAU header. If the ICAUVer broadcast in the PACAU header is later than that which the IPoS remote already has, the IPoS remote should make an ICAU Request (after waiting a random backoff time) via the telephone line that must be connected to the IPoS remote in order to make this request. The ICAU Request is defined in table 4.20-1.

The ICAU-R may contain a mixture of EKs and GKs, in which the ICAU-R's Payload Group ID field value will be equal to 0xFF for the EK. See table 4.13.10-1.

Table 4.13.10-1. ICAU Request

Field Name	Field Length (bits)	Description
Reserved	8	Set to 0x05
Serial Number	24	IPoS remote's serial number in hex, LSB first.
Reserved	32	Reserved
Reserved	32	Reserved
Signature	64	Signature of complete ICAU-R inclusive of timestamp. Does not include any bit-stuffing required.

The response to an ICAU Request, termed the ICAU-R, is contained in table 4.13.10-2.

Table 4.13.10-2. ICAU Response Header

Field Name	Field Length (bits)	Description
Reserved	8	Shall be value 0x01
Reserved	8	Shall be value 0x00
Reserved	16	Reserved

Table 4.13.10-2. ICAU Response Header

Field Name	Field Length (bits)	Description
Signature	64	Contains the Signature field from the corresponding ICAU Request. The IPoS remote shall compare the two signatures to ensure that the ICAU-R is not directed at another IPoS remote.
ICAU Version Number	32	Hold ICAUVer number, LSB first.
Number of Entries	32	Hold the Number of Entries that follow. Each entry contains the following fields: Group ID, Group Version Number, and Group Control Word. The maximum number of entries is 250.
EEMK	128	EEMK for this IPoS remote

Table 4.13.10-3 shows the entry format for ICAU GK.

Table 4.13.10-3. ICAU Group Key Entry Format

Field Name	Field Length (Bits)	Description
GroupID	24	Unique GroupID
Version	8	Current crypto Version
Crypto Key	64	Crypto Key

Table 4.13.10-4 shows the entry format for ICAU EK.

Table 4.13.10-4. ICAU Element Key Entry Format

Field Name	Field Length (Bits)	Description
ElementID	24	Set to 0xFF
Version	8	Current crypto Version
Crypto Key	64	Crypto Key

4.13.11 Periodic Element Broadcast (PEB)

The hub periodically sends the PEB command providing mapping information that shall be used by the IPoS terminal to map encrypted multicast encryption keys to MAC addresses sent over the unicast conditional access channel. The fields and meanings in the PEB are given table 4.13.11-1.

Table 4.13.11-1. PEB Format

Field Name	Field Length (bits)	Description
VersionNumber	32	VersionNumber of PEB
GroupID	24	GroupID of which this element is a member

Table 4.13.11-1. PEB Format

Field Name	Field Length (bits)	Description
GroupVersion	8	Crypto version of the group
Number of Entries	16	This field contains the number of MACAddresses to which the PEB applies.
MACAddress	Nx48	This field contains all the MAC addresses to which the PEB applies. N is defined by the value of the Number of Entries field.

4.14 Configurable Parameters

The remote terminal needs to have the following data configured locally as part of its commissioning procedure before it can acquire an outroute and send data:

- Outroute:
  - Frequency
  - Symbol rate
  - Coding rate
  - Modulation type
  - Valid outroute groups for this terminal
- Satellite longitude
- Longitude and latitude of terminal site
- IP address of IP packet processor at the hub
- Its own internal IP address within the system

The hub must have the encrypted keys configured for every IPoS terminal with which it will operate and for every multicast stream.

ANNEX A - (NORMATIVE): STATE MACHINES

This annex shows state machines and message sequence diagrams for several of the processes that IPoS remote terminals execute. These are logical state diagrams that are intended to illustrate functions; they do not imply a particular implementation.

A.1 Superframe Synchronization

A.1.1. State Diagram

Figure A.1.1-1 and the flowcharts in the following subsections show the states and transitions that embody the superframe synchronization logic that is described in subsection 4.10.1.4.3. When the terminal acquires or loses superframe synchronization, it sends a corresponding event to the main remote terminal state machine that is described in section A.2 of this annex.

Under normal conditions, after the terminal starts, the following sequence of events occurs:

1. The terminal enters the Waiting for 1st SFNP state.

2. After some period of time, the terminal receives its first SFNP. The terminal advances to the Waiting for 2nd SFNP state.

3. The terminal receives its second SFNP. If the number on this SFNP indicates that it is the next SFNP sequence, the terminal advances to the Waiting for 3rd SFNP state. Instead, if the timeout occurs (about 361 msec after the first SFNP was received), this indicates that the next SFNP was missed and the terminal returns to the Waiting for 1st SFNP state.

4. The terminal receives its third SFNP, and the sequence number is the next one expected. The terminal advances to the Waiting for 4th SFNP state.

5. The terminal receives its fourth SFNP, and the sequence number is the next one expected. Also the hub timing is within eight clock ticks of the remote terminal's timing. The terminal enters the Sync'ed-to-Superframe state and sends a Superframe Sync event to the Main Terminal state machine.

The flowcharts in subsections A.1.2 and A.1.3 show how synchronization events are processed in the Sync'ed-to-Superframe state.

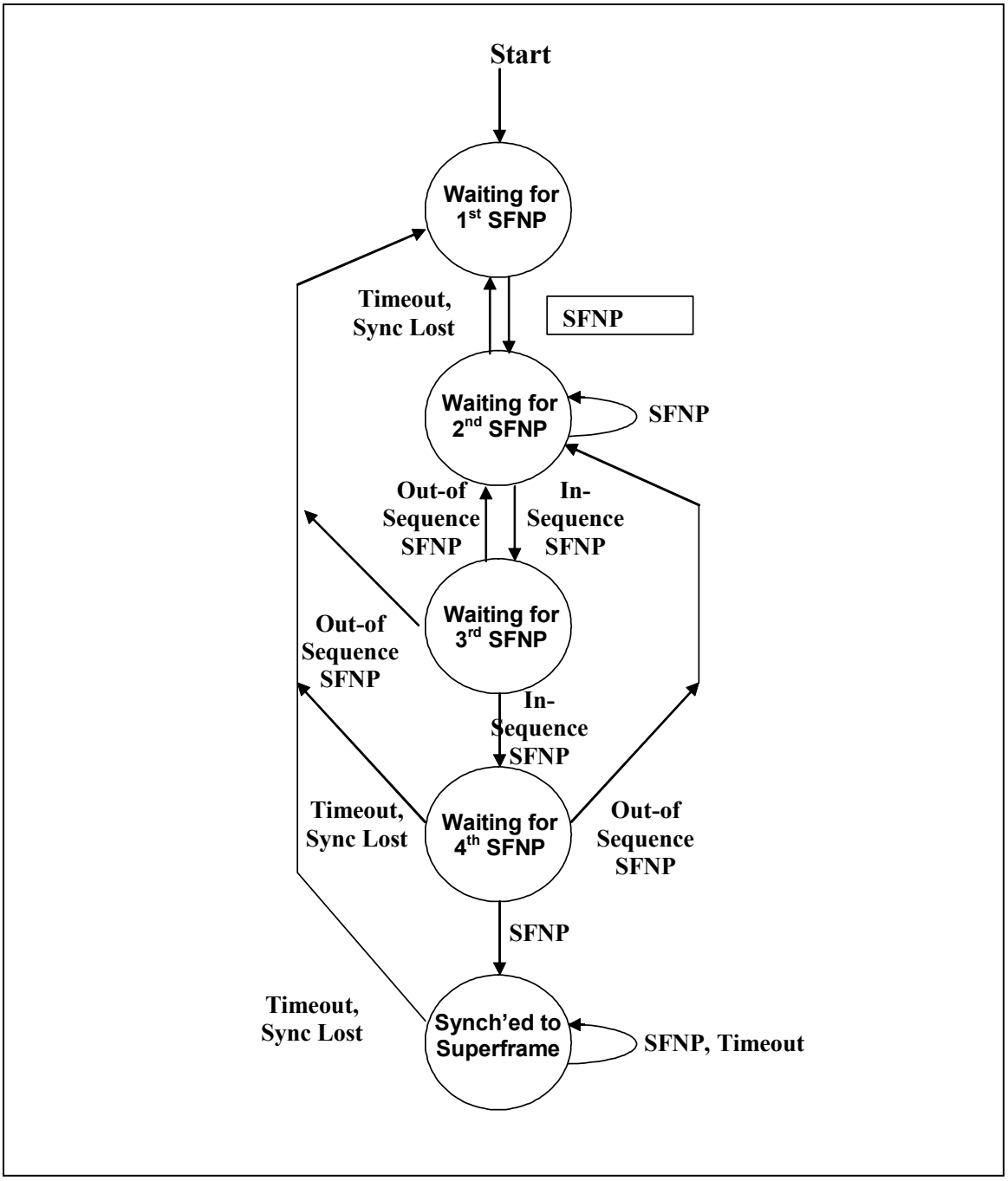


Figure A.1.1-1. IPoS Terminal Superframe Timing States

A.1.2 SFNP Processing in Sync'ed-to-Superframe State

Figure A.1.2-1 shows the processing in the Sync'ed-to-Superframe state when the terminal receives an SFNP. Typically this will be the next SFNP in sequence. The terminal sets the 2-out-of-5 counter to zero indicating that it has been

0 frames since two sequential SFNPs have been received. Furthermore, if this is the 3rd SFNP that has been received in sequence, the terminal sets the 3-out-of-7 counter to zero to indicate that it has been 0 frames since three sequential SFNPs have been received.

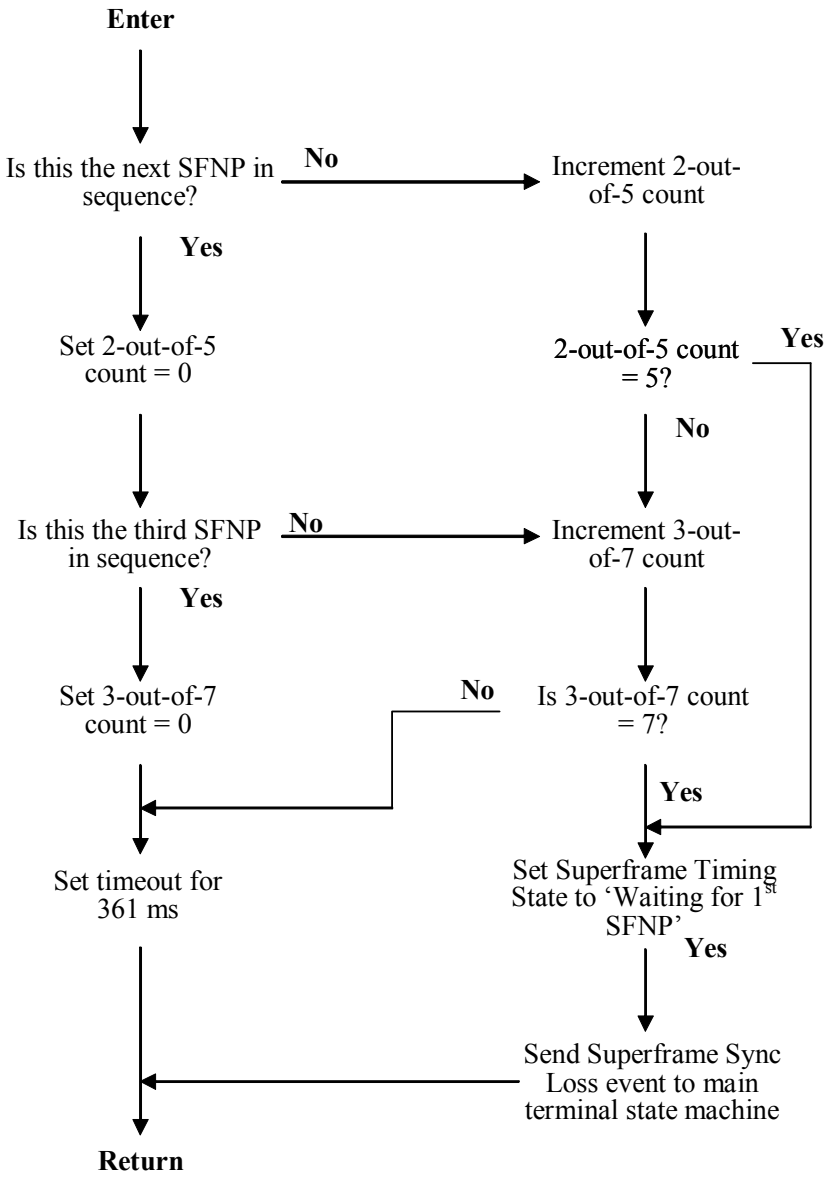


Figure A.1.2-1. Processing for SFNP in Sync'ed-to-Superframe State

A.1.3 Timeout Processing in Sync'ed-to-Superframe State

Figure A.1.3-1 shows the processing for a timeout received in the Sync'ed-to-Superframe state. The timeout is set for 361 msec, 1 msec longer than the superframe interval, so a timeout indicates that an SFNP was missed.

For a missed SFNP timeout, the terminal increments both the 2-out-of-5 and 3-out-of-7 counters to indicate the number of frames missed. If the number of frames missed now meets either criterion for superframe sync loss, the state machine sends a sync loss event to the main terminal state machine. Otherwise, the terminal waits for the next superframe interval. See Figure A.1.3-1.

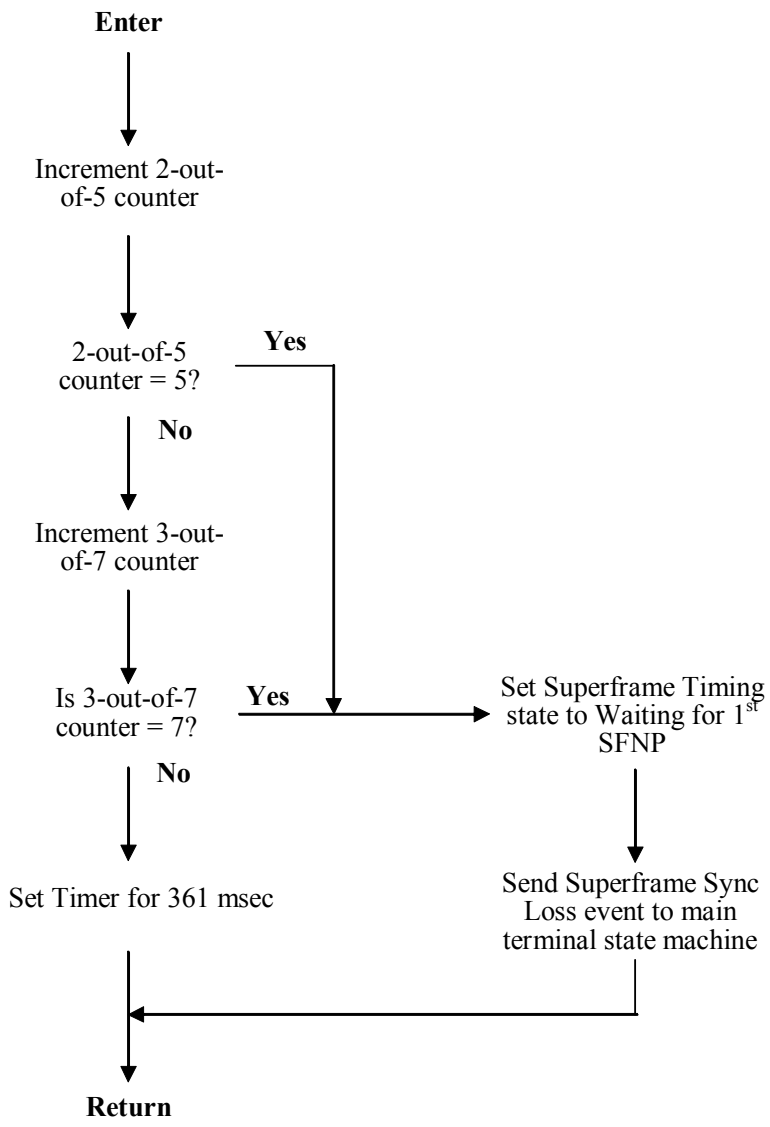


Figure A.1.3-1. Processing for Superframe Timeout in Superframe State

A.2 Remote Terminal Operating States

A.2.1 Normal Operation

This subsection describes the event/state processing for the case where there are no errors or failures. Figure A.2.1-1 shows the remote terminal states.

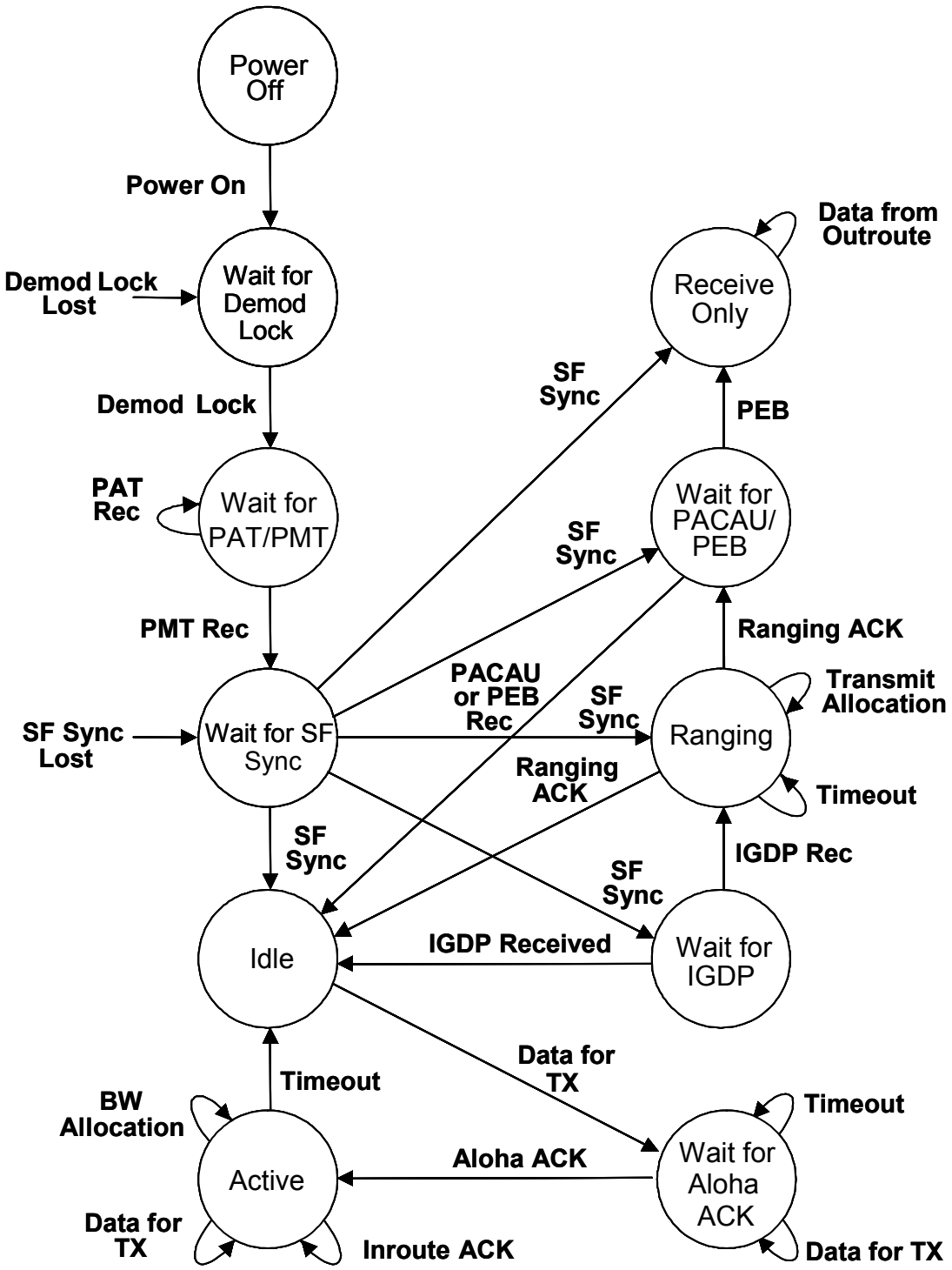


Figure A.2.1-1. IPoS Remote Terminal State Diagram

Assuming that a terminal has already been commissioned, received its encryption keys, and ranged, a terminal might perform the following functions when power is applied:

1. Enter the frequency and modulation parameters for the demodulator (see subsection A.2.2).

2. Enter the Wait for Demod Lock state.

3. After a few seconds, the demodulator locks onto the outroute, and the terminal enters the Wait for PAT/PMT state (see subsection A.2.3).

4. The terminal receives the DVB PAT (Program Association Table) message. From the PAT the terminal determines which PID is listed to receive the PMT (Program Map Table) DVB message (see subsection A.2.4).

5. The terminal receives the PMT message and determines the PIDs to be used for IPoS control messages and data. The terminal sets the hardware to receive data from these PIDs and enters the Wait for SF Sync state (see subsection A.2.5).

6. While it is in the Wait for SF Sync state, the terminal processes both SFNPs and IGDPs that it receives (see subsections A.1 and A.2.6). During this time, the Superframe Synchronization state machine runs independently of the terminal's high-level state machine.

7. The terminal receives a sufficient number of consecutive SFNPs to declare that superframe synchronization has been acquired. The terminal enters the Idle state (see subsection A.2.7). In this state the terminal sends any IP packets that it receives from the outroute that are addressed to the terminal (either by unicast or multicast) through the SI-SAP to the layer above the DLC layer.

8. When the terminal sends an IP packet through the SI-SAP to the DLC layer for transmission, the terminal uses the inroute group selected during idle. The inroute group must have one or more Aloha request channels.

9. The terminal sends an Aloha request for bandwidth along with the first part of the IP packet to be sent to the hub and enters the Wait for Aloha ACK state (see subsection A.2.8).

10. The terminal receives an Aloha Ack message and enters the Active state (see subsection A.2.9).

11. The terminal receives successive BAPs.

12. The terminal transmits the remaining IP data, including new IP packets that may have come in since the first one (see subsection A.2.10).

13. The terminal runs out of data and stops sending IP data. However, it must send idle bursts for any allocations that it receives.

14. The terminal has no data to transmit and receives a configurable number of consecutive frames without receiving a bandwidth assignment (see subsection A.2.11).

15. The terminal enters the Idle state.

A.2.2 Enter Wait for Demod Lock State

Figure A.2.2-1 shows the processing executed when the remote terminal starts up or after it has lost demod lock. The terminal initializes its data buffers and address filters and waits for the demodulator to lock to the outroute.

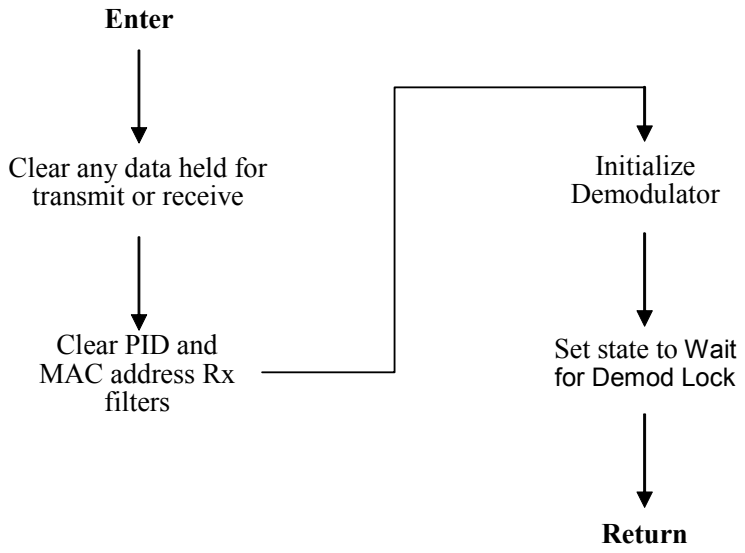


Figure A.2.2-1. Processing for Entering the Wait for Demod Lock State

A.2.3 Demod Lock Received in Wait for Demod Lock State

Figure A.2.3-1 shows the processing executed when the remote terminal receives demodulator lock when it is in the Wait for Demod Lock state. The terminal sets the receive filter to PID 0, the DVB PID on which PAT and PMT messages are sent. Then the terminal enters the Wait for PAT/PMT state for the first PAT message.

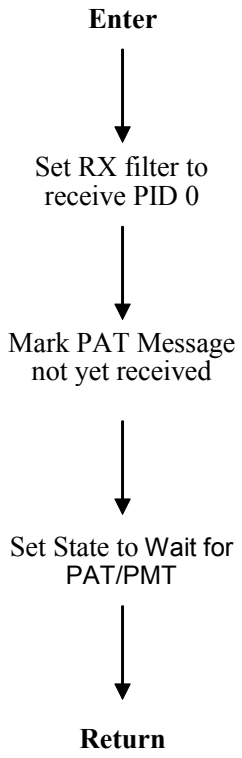


Figure A.2.3-1. PAT Message Processing in the Wait for PAT/PMT State

A.2.4 PAT Message Received in Wait for PAT/PMT State

Figure A.2.4-1 shows the processing executed when the remote terminal receives a PAT message while it is in the Wait for PAT/PMT state. The PAT message gives the terminal the value of the PID on which it should expect to receive the PMT message. The terminal sets its receive filter to process this PID.

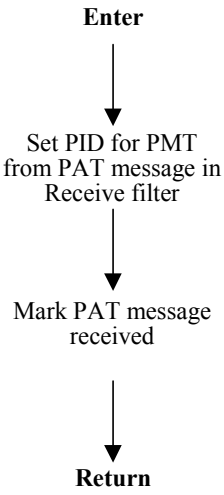


Figure A.2.4-1. PAT Message Processing in the Wait for PAT/PMT State

A.2.5 PMT Message Received in Wait for PAT/PMT State

Figure A.2.5-1 shows the processing executed when the remote terminal receives a PMT message while it is in the Wait for PAT/PMT state. The PMT message gives the terminal the PIDs to use for IPoS data and control messages, and the terminal sets its receive filter to process these PIDs. If the keys have already been received, the terminal installs them in the decryption device. The terminal then sets the state in the Superframe Synchronization state machine (see subsection A.1) to Wait for SF Sync to begin the process of establishing superframe synchronization.

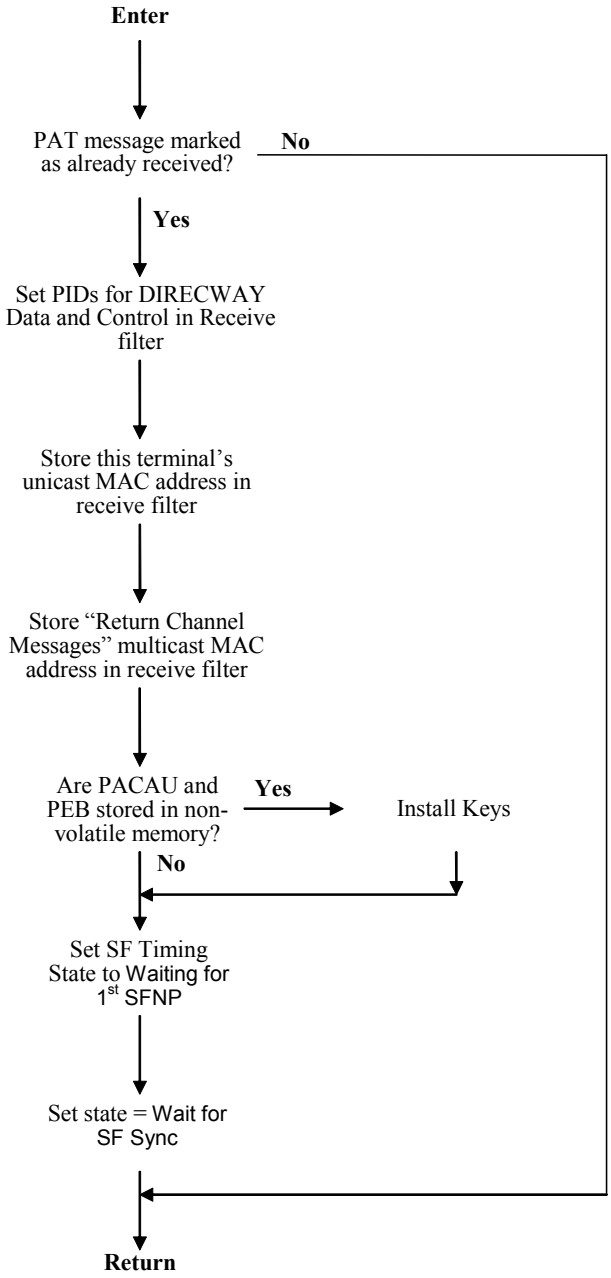


Figure A.2.5-1. PMT Message Processing in the Wait for PAT/PMT State

A.2.6 IGDP Message Received in Wait for SF Sync State

Figure A.2.6-1 shows the processing executed when the remote terminal receives an IGDP message while it is in the Wait for SF Sync state. The terminal saves any new inroute group information that the message may contain.

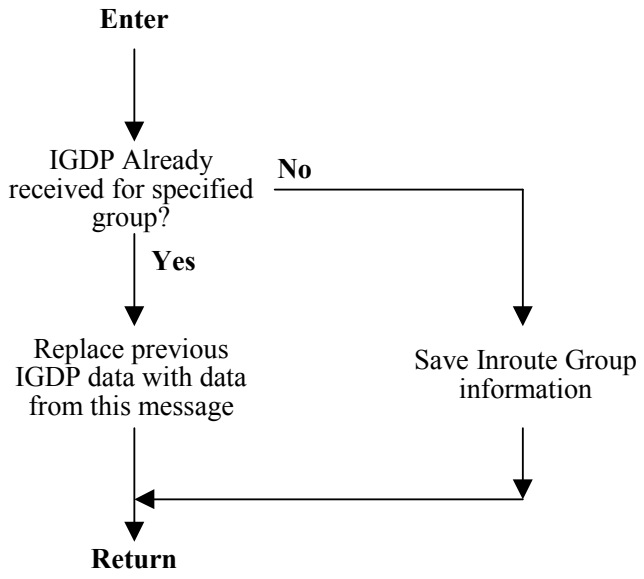


Figure A.2.6-1. Process IGDP Message Received in the Wait for SF Sync State

A.2.7 SF Sync Event Received in the Wait for SF Sync State

Figure A.2.7-1 shows the processing executed when the terminal goes into superframe synchronization (see subsection A.1) when it is in the Wait for SF Sync state. Typically, the processing follows the main line of processing to the left of the figure, and the terminal enters the Idle state.

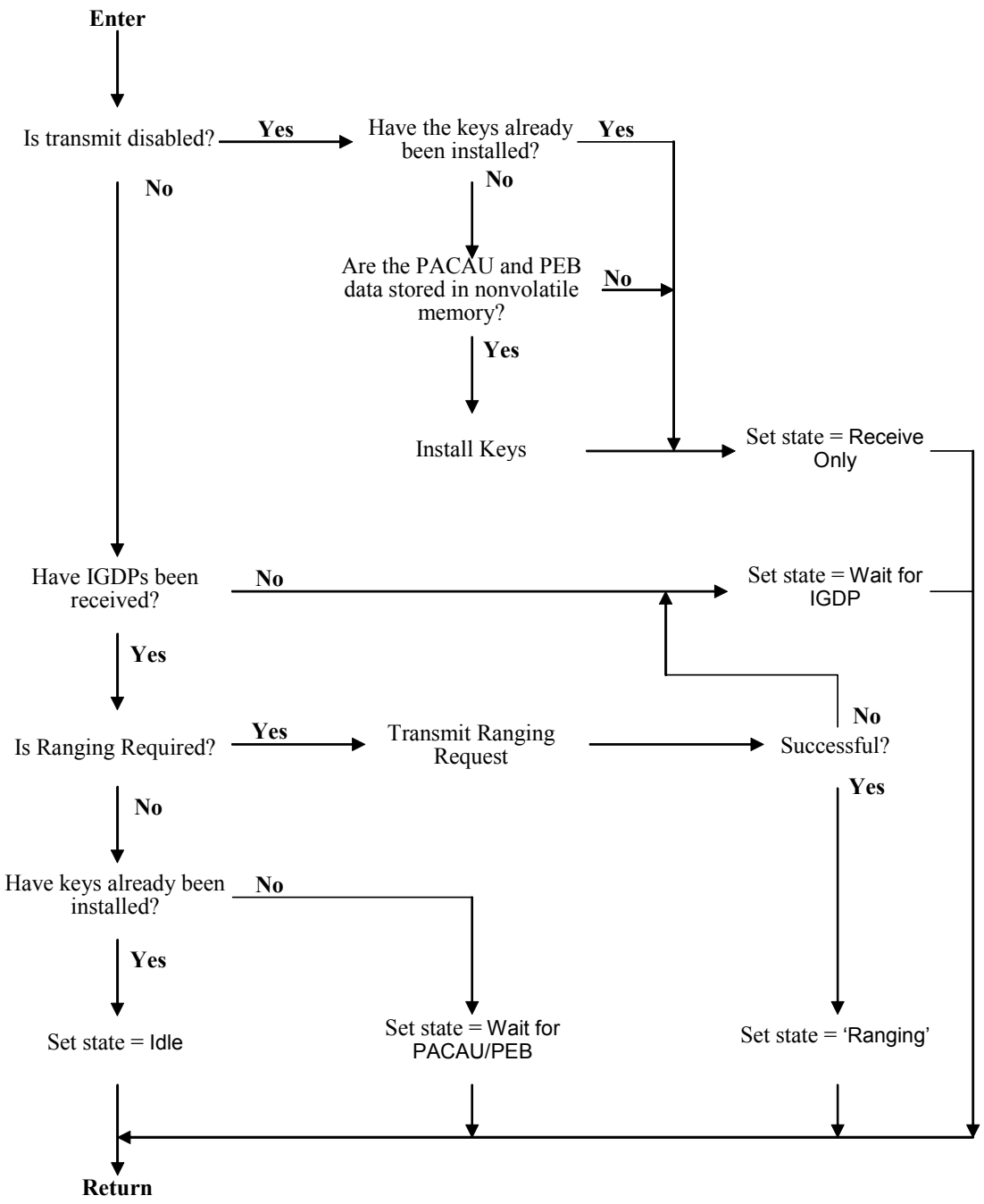


Figure A.2.7-1. Process SF Sync Event in the Wait for SF Sync State

A.2.8 IP Data for Transmission Received in Idle State

Figure A.2.8-1 shows the processing executed when the terminal receives IP data for transmission on the inroute when it is in the Idle state. The terminal chooses two Aloha slots, sends a Bandwidth Request message on each of the chosen slots, then enters the Waiting for Aloha ACK state.

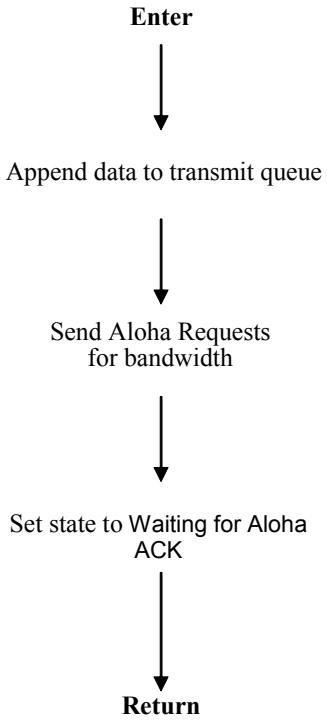


Figure A.2.8-1. Process Data for Inroute Transmission Received in Idle State

A.2.9 Aloha ACK Message Received in Wait for Aloha ACK State

Figure A.2.9-1 shows the processing executed when the terminal receives an Aloha ACK message while it is in the Wait for Aloha ACK state. Typically, the processing follows the main line of processing to the left of the figure, and the terminal enters the Active state.

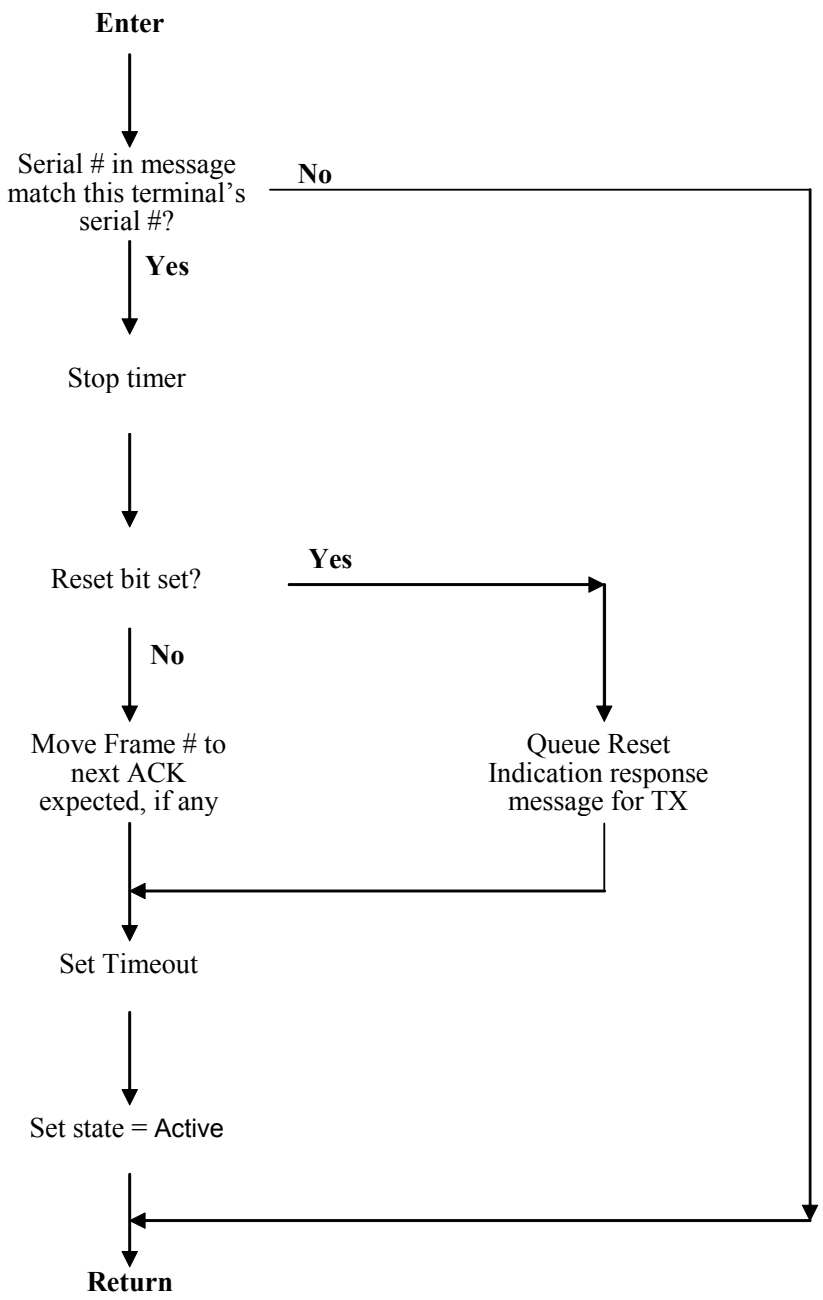


Figure A.2.9-1. Process Aloha ACK Received in Wait for Aloha ACK State

A.2.10 Bandwidth Allocation Message Received in Active State

Figure A.2.10-1 shows the processing executed when the terminal receives a Bandwidth Allocation message when it is in the Active state. If the terminal has data to be transmitted, it transmits it in the assigned slots. If it has no data to transmit, it transmits a null burst in the assigned slots.

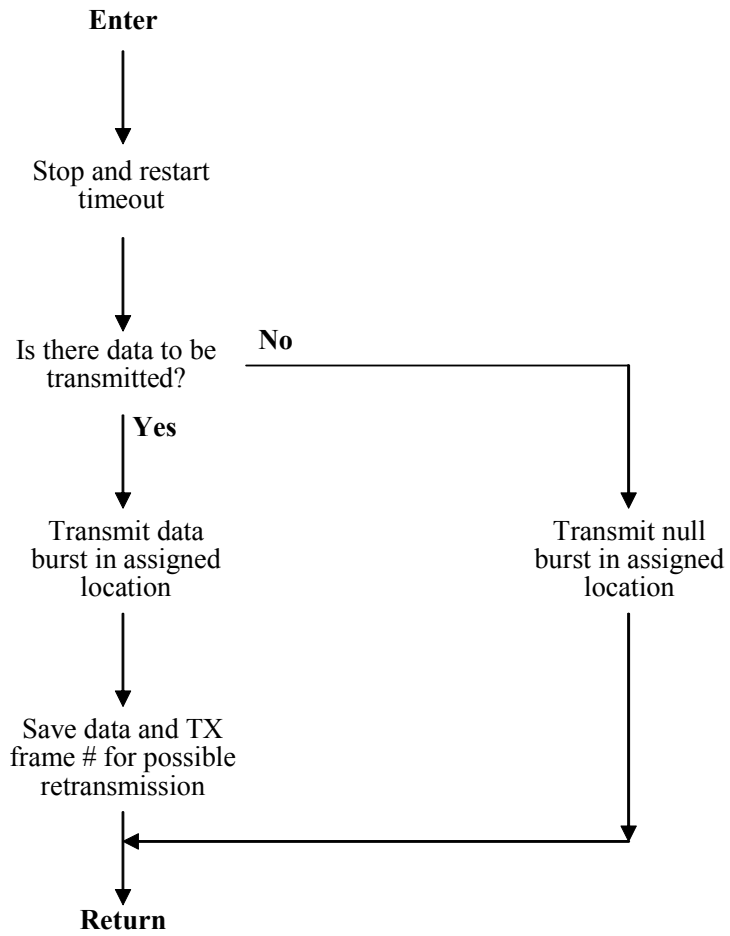


Figure A.2.10-1. Process Bandwidth Allocation Message Received in Active State

A.2.11 Timeout in Active State

Figure A.2.11-1 shows the processing executed when the terminal receives a timeout (a configurable number of consecutive frames without a bandwidth allocation) when it is in the Active state. If the terminal has data to be transmitted, it must become active again by sending an Aloha Request message. Otherwise, the terminal removes the MAC address for the current outroute group from the terminal's receive filter so that it will not have to process extraneous bandwidth assignment and other messages.

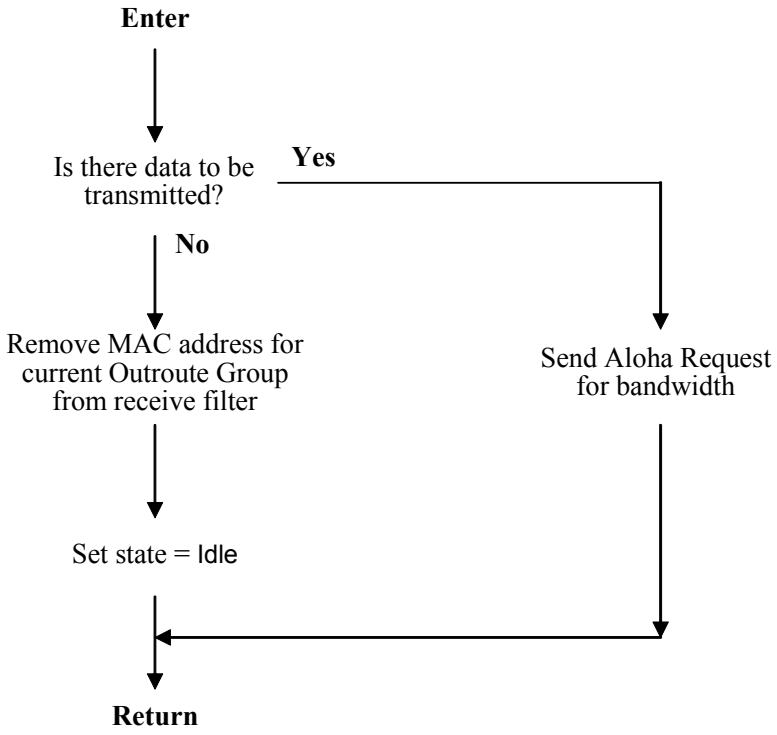


Figure A.2.11-1. Process Timeout in the Active State

This page intentionally left blank.

ANNEX B- IPOS SECURITY

B.1 Scope

This document is an annex to the IP over Satellite (IPoS) MAC/SLC Layer Specification that describes the security procedures supported within IPoS.

The purpose of security is to prevent unauthorized access to IPoS services. In order to fulfill this goal, the following features are supported:

- Provision for the secure transfer of information to the IPoS subscriber.
- Provision of secure means for conveying management and control information.
- Protection of revenues from the IPoS system.

The IPoS security architecture relates to the outroute direction between the IPoS hub and the IPoS remote terminals. The architecture contains management, control, and user plane procedures providing the following security services:

- Protection of the privacy of the content of unicast outroute transmissions.
- Control of access to multicast services.
- Prevention of unicast reception by unauthorized receivers.

End-to-end service protection extending from the user to the service provider might be provided on top of satellite IPoS security by a separate mechanism, typically IPsec.

B.2 Security System Architecture

B.2.1 Introduction

The IPoS security architecture relies upon:

- Decryption keys that only unlock various IPoS services to a database of authorized users. There is a hierarchy of encryption keys, which includes key encrypting and keys for protecting the information sent from the hub to the remote terminals.
- Procedures for the distribution and update of the keys needed at the IPoS hub and IPoS remote terminals prior to the encryption/decryption of information.
- The actual encryption/decryption of keys, control, and user information sent over the outroute direction.

B.2.2 Database of Authorized Users

IPoS authentication is based on a shared-key scheme where the hub has knowledge of information derived from a master key (MK) (the effective master key, EMK) stored at each remote terminal. The hub's information allows the secure distribution of key material to an IPoS remote.

The binding between the remote terminal's MK and the hub's key information normally takes place during the commissioning of the terminal. During the registration procedure, the parameters such as hardware serial number, customer name, and contact information, which identify the remote terminal, are sent to the IPoS hub out-of band. Once received, the information is stored at the hub and associated with the EMK information that allows the identification of remote terminals.

From these parameters, the hub's security management entities can determine the services and types of keys required by each remote terminal as well as the MAC address associated with the remote terminal over the IPoS remote.

Security management entities at the hub create the appropriate messages with the keys that will be distributed to the remote terminals over the outroute direction.

The terminal demonstrates its identity by its knowledge of this MK. This MK allows the terminals to decrypt the messages sent by the hub with the keys that will be used to encrypt the information of the various services.

The encryption keys are changed periodically to limit the period in which a service is exposed to security breaches. Authorization to receive services is revoked at the hub by withholding from a remote the updated keys needed to decrypt the services.

B.2.3 Key Hierarchy

The IPoS security architecture uses a three-layer key hierarchy, which allows effective management, control, and update of key information for each remote terminal. The partition of keys into these three layers reduces the complexity of the IPoS security architecture. In this architecture the keys in the "upper" layers protect the keys in the "lower" layers, thus increasing the flexibility and security of the system. The three layers of security architecture are illustrated in figure B.2.3-1.

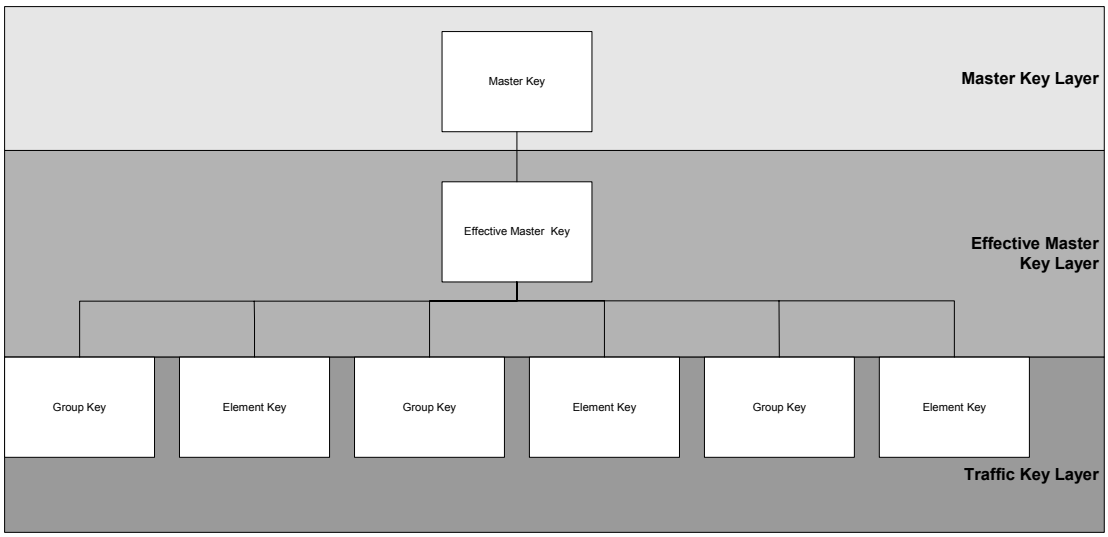


Figure B.2.3-1. IPoS Security Key Hierarchy

The two upper layers of the key hierarchy contain key-encrypting keys that are used to encrypt the keys of the layer below, e.g., the EMK layer is encrypted under the MK layer and the traffic key (TK) layer is encrypted with the EMK layer. The key-encrypting keys in the MK and EMK layers are 192 bits wide, which are obtained with a triple-DES encryption/decryption operation where each of the 192-bit wide keys consists of three 64-bit blocks of the standard single DES 64-bit block key. The group key (GK) and element key (EK) in the lower TK layer are 64 bits wide and are used to protect user traffic with a single DES block.

Each layer has keying material, key distribution, and management procedures pertaining to it. These are specified in the following subsections.

B.2.3.1 Master Key Layer

The MK layer is the highest level of IPoS security architecture. Every key in the MK layer is unique to each IPoS remote. The MK is a key-decrypting key that decrypts the EMK. The MK is never used to encrypt or decrypt user traffic.

B.2.3.2 Effective Master Key Layer

The EMK resides at the EMK layer. The EMK is specific to each IPoS remote. The EMK is a key-decrypting key. The EMK decrypts TKs that are assigned to that IPoS remote or multicast group. The EMK is never used to encrypt or decrypt user traffic.

B.2.3.3 Traffic Key Layer

There are two keys resident at the TK layer: the GK and the EK. The GK is used to encrypt data that is addressed to multiple IPoS remotes in multicast groups; the EK is used to encrypt data that is addressed to an IPoS remote's unicast address.

Each multicast group has its own key material; therefore, each GK is specific to an IPoS multicast group. The GK decrypts multicast traffic for a specific multicast group on the IPoS outroute.

The EK is associated with IPoS elements. An IPoS element is the smallest unit of data that can be controlled by the IPoS security system. IPoS elements are usually associated with IPoS services. For example, an Internet surfing service can be viewed as an element. Unicast user's data is encrypted under the EK on the IPoS outroute.

B.2.4 Key Creation

B.2.4.1 Master Key Layer

The MK is created at a separate key creation facility. This facility is normally a secure facility in close proximity to the manufacturing location of the IPoS remotes.

A single MK is loaded into an IPoS remote by a secure key-loading device. The key-loading device protects the security of the MK by not allowing the keys to be loaded in any other remote than the target IPoS remote.

Each MK is unique to a single IPoS remote.

To guard the security of the MK, the MK is loaded in a secure register at the remote terminal such that the IPoS remote shall never reveal the value of the MK.

B.2.4.2 Effective Master Key Layer

As part of the key creation process, EMKs for each remote are created.

The EMKs are used to make the encrypted effective master key (EEMK).

The EEMK is created by the separate key creation facility. To create an EEMK, the separate key creation facility uses one EMK (for the remote that will eventually receive the EEMK) and then encrypts the EMK with the target IPoS remote's MK. The EMK and associated EEMK are paired together then stored at the IPoS hub.

The advantage of this system is that, should the key material stored in the IPoS hub become compromised, the IPoS remote can be rekeyed with another EMK, re-establishing the integrity of the IPoS security system. Therefore, the terminal's manufacturer is exclusively responsible for maintaining the security of the terminal's MK

The EEMK can be transmitted from the IPoS hub to the IPoS remote within a PACAU or ICAU packet (see subsection 4.5 for details of these packets).

The MK is used by the IPoS remote to decrypt the EEMK. The result of decrypting the EEMK with the MK is the EMK, thus securely establishing the

EMK as the shared secret between the IPoS hub and IPoS remote. The EMK is used to encrypt the TKs at the IPoS hub and to decrypt them at the IPoS remote. Therefore, the hub uses a remote's EMK to encrypt the TKs required for the services the remote terminal is authorized to receive. The remote terminal uses its EMK to decrypt the TKs and thus gain access to those services.

This process is illustrated in figure B.2.4.2-1.

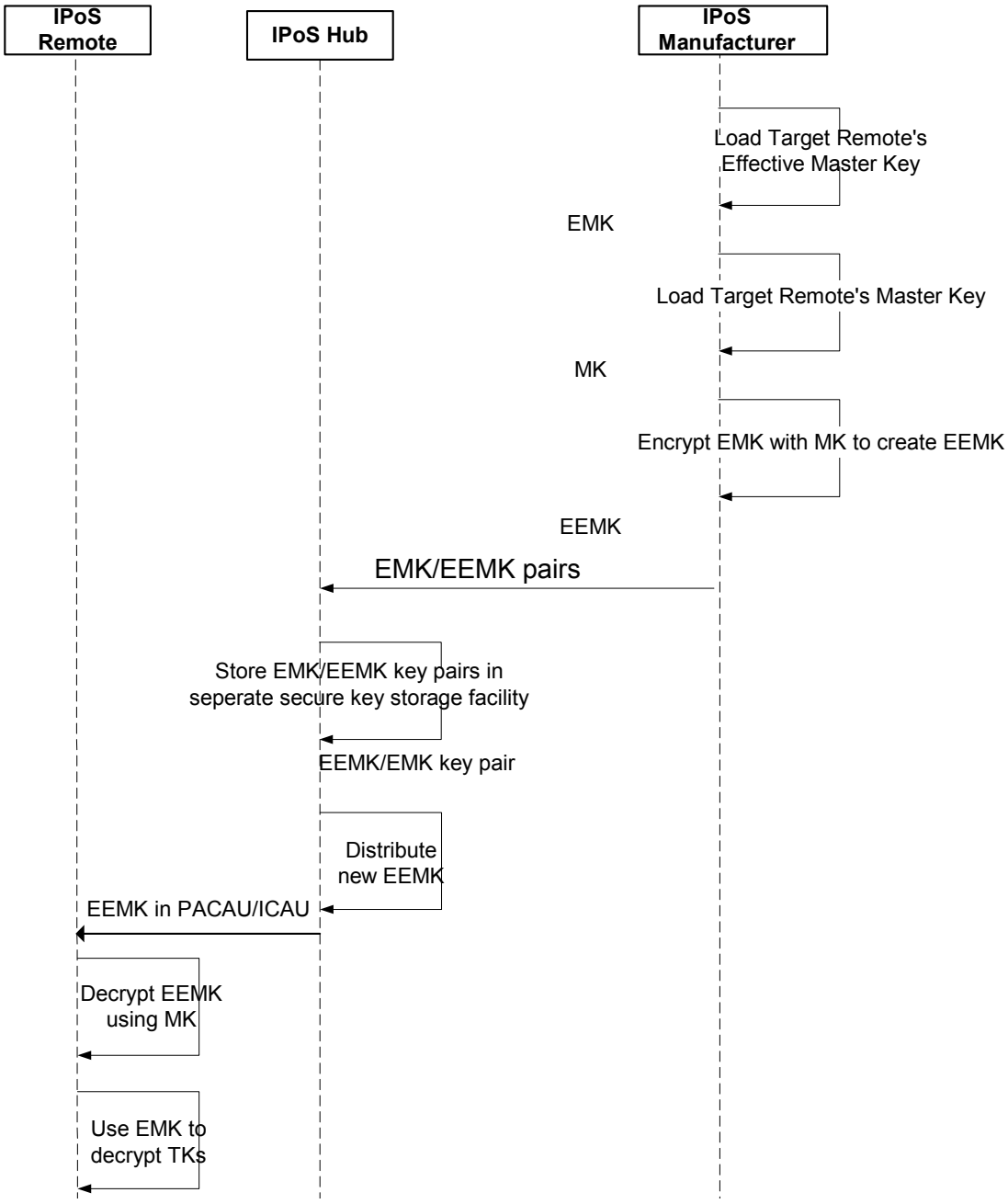


Figure B.2.4.2-1. EEMK Distribution Procedure

B.2.4.3 Traffic Key Layer

The GKs for each remote are created at the IPoS hub. A GK for each multicast group will be created and encrypted under the target IPoS remote's current EMK to create the encrypted group key (EGK).

Upon reception of the EGK, the IPoS remote shall decrypt the EGK with its current EMK to create the GK. Upon success, the GK can be used to decrypt multicast data feeds that will be addressed to the remote terminals at the address expressed in the Periodic Element Broadcast (PEB) packet.

This process is illustrated by figure B.2.4.3-1.

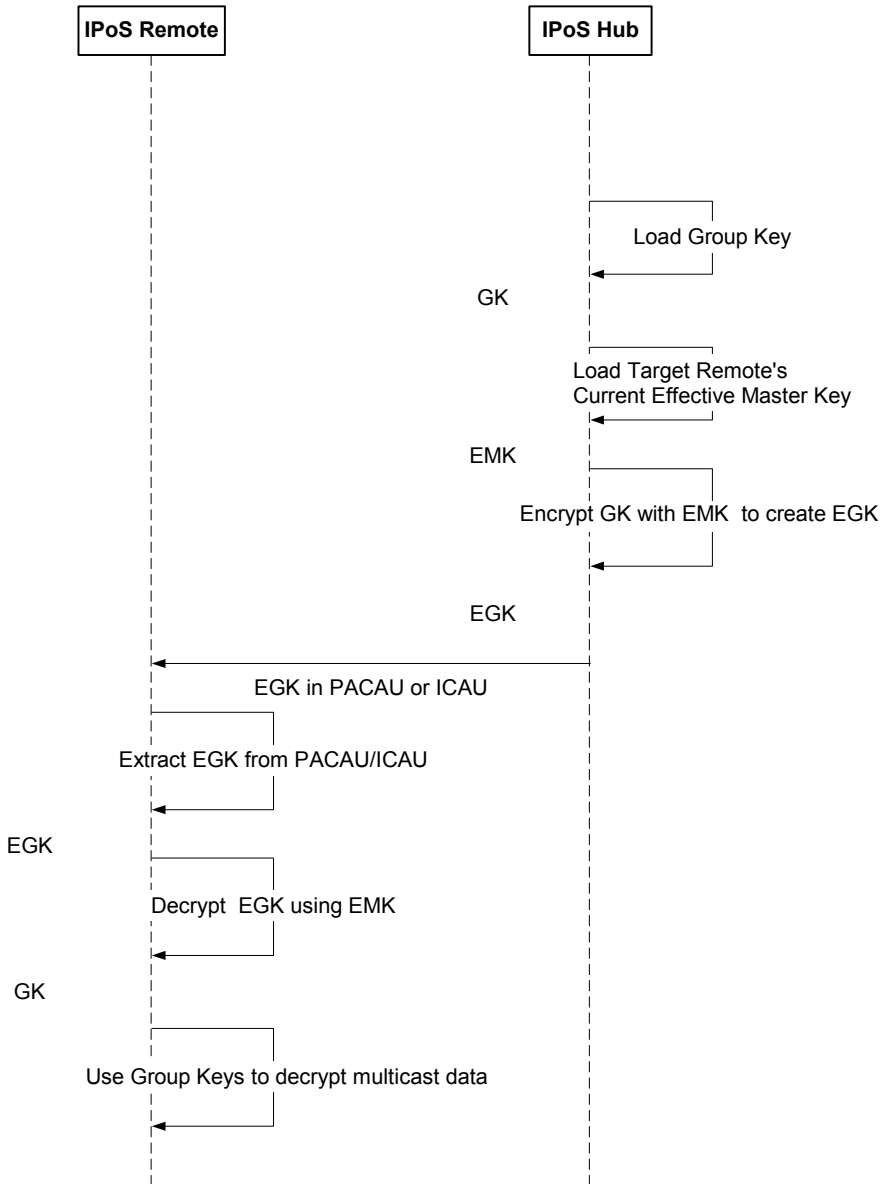


Figure B.2.4.3-1. Group Key Creation and Distribution Procedure

Each IPoS unicast data feed has its own key material. This key material is called an EK. Each EK is specific to an IPoS unicast data feed.

Once these keys have been created, they are encrypted under the target remote terminal's EMK. The result of this encryption is the EEK.

The EEK is transmitted to the IPoS remote in PACAU or ICAU packets.

Upon reception of the EEK, the IPoS remote shall decrypt the EEK with its current EMK to create the EK. Upon success, the resultant EK can be used to decrypt unicast user traffic that will be addressed to the IPoS remote.

This process is illustrated by figure B.2.4.3-2.

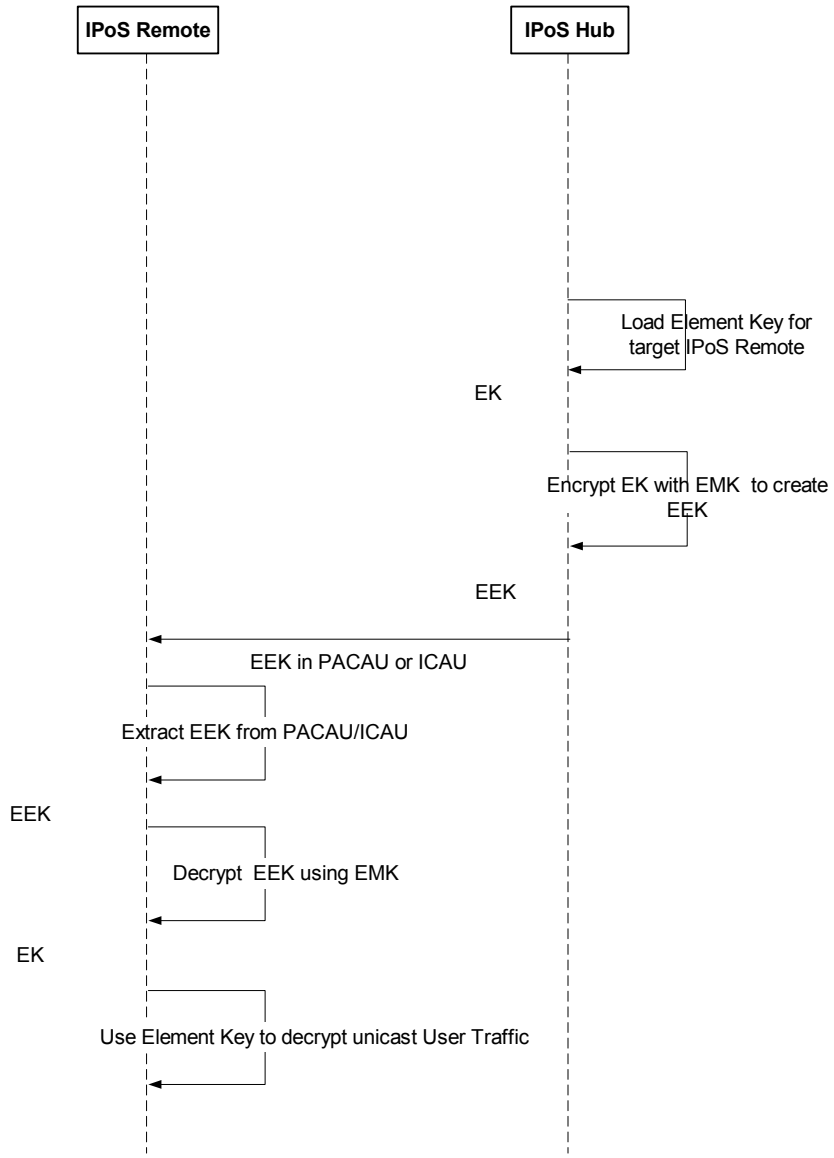


Figure B.2.4.3-2. Element Key Creation and Distribution Procedure

B.2.4.4 Key Association Summary

Table B.2.4.4-1 summarizes the encryption of the various keys in the IPoS security architecture and their association with the different layers.

Table B.2.4.4-1. Encryption of Keying Association with Each Layer

Layer	Key	Encryption Key	Product of Encryption	Site of Encryption	Packet Used
Master	MK	N/A	N/A	N/A	N/A
Effective Master	EMK	MK	EEMK	Remote Terminal Manufacturing Site Separate Key Creation Facility	PACAU ICAU
Traffic	EK	EMK	EEK	Hub	PACAU ICAU
	GK	EMK	EGK	Hub	PACAU ICAU

Table B.4.4.4-2 summarizes the decryption processes associated to the various keys.

Table B.2.4.4-2. Decryption of Keying Association with Each Layer

Layer	Key	Decryption Key	Product of Decryption	Packet Used
Master	MK	N/A	N/A	N/A
Effective Master	EEMK	MK	EMK	PACAU ICAU
Traffic	EEK	EMK	EK	PACAU ICAU
	EGK	EMK	GK	PACAU ICAU

B.2.5 Key Distribution

B.2.5.1 Introduction

In IPoS, encryption keys are distributed by the hub employing two types of messages: the PACAU and ICAU. Another message, the PEB, carries the MAC addresses of each multicast group. The packet types and their functions will be described within this subsection.

B.2.5.2 Periodic Adapter Conditional Access Update Description

The PACAU consists of a header, EEMK, EGKs, and EEK, which the targeted IPoS remote requires for its authorized services. Subsection 4.13.9 defines the PACAU header format and the PACAU payload format for GKs and EKs.

The PACAU is individually addressed to each IPoS remote using its unicast MAC address, which is unique to every IPoS remote. Only the IPoS hub can

create and send a PACAU. Figure B.2.5.2-1 shows the creation and distribution of the PACAU.

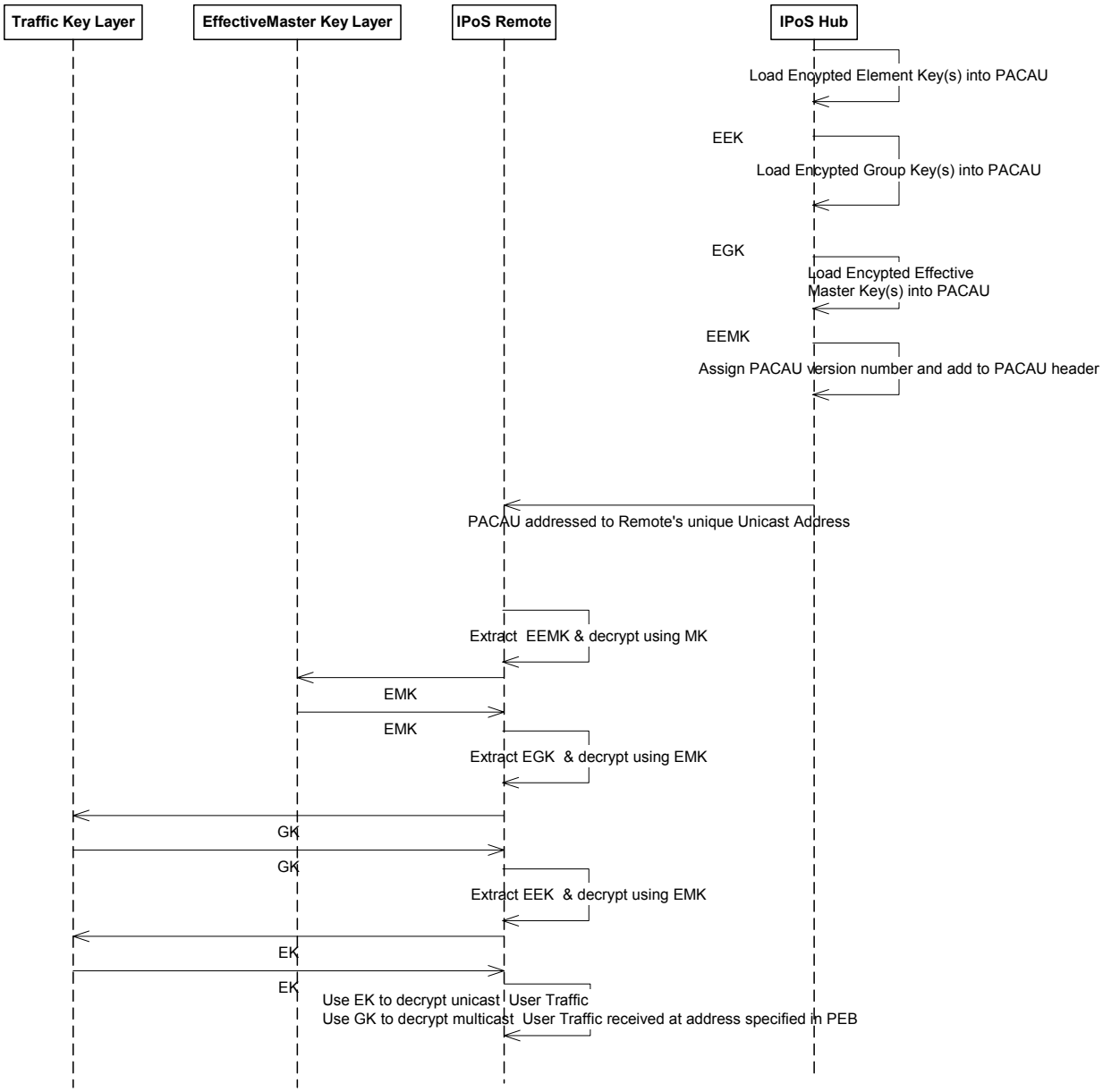


Figure B.2.5.2-1. PACAU Creation, Distribution, and Association of Keying with Layers

B.2.5.3 Interactive Adapter Conditional Access Update Description

The ICAU is sent to an IPoS remote during commissioning to initially provide the IPoS remote with its keys and is also sent when the IPoS remote requests an updated ICAU (using the ICAU Request) from the IPoS hub. The ICAU Request is created when the IPoS remote realizes that its ICAU is out of date and so requires an update (see subsection B.2.5.5 for update procedures). The ICAU Request includes a signature from the IPoS remote that is unique to that remote and that request. (This signature is formed using a process that is critical to the security of IPoS: therefore, the definition of this signature is only made available to licensed manufacturers.) Once the ICAU Request has been authenticated by the IPoS hub, an ICAU Response (ICAU-R) to the IPoS remote is made. The ICAU-R is individually addressed to each IPoS remote and includes the signature from the ICAU Request. To authenticate the ICAU-R, the signature must match that used in the ICAU Request; otherwise, the ICAU-R is ignored.

Both the ICAU Request and ICAU-R are sent “out-of-band” only (i.e., not via the IPoS inroute or outroute). Only the IPoS hub can create and send a valid ICAU-R as only it has access to the EEMK that forms a part of it.

In total, the ICAU-R consists of a header, EEMKs, EGKs, and EEKs, which the targeted IPoS remote requires for its authorized services. Subsection 4.13.10 defines the ICAU Request format and the ICAU-R format.

Figure B.2.5.3-1 illustrates the ICAU Request and ICAU-R process.

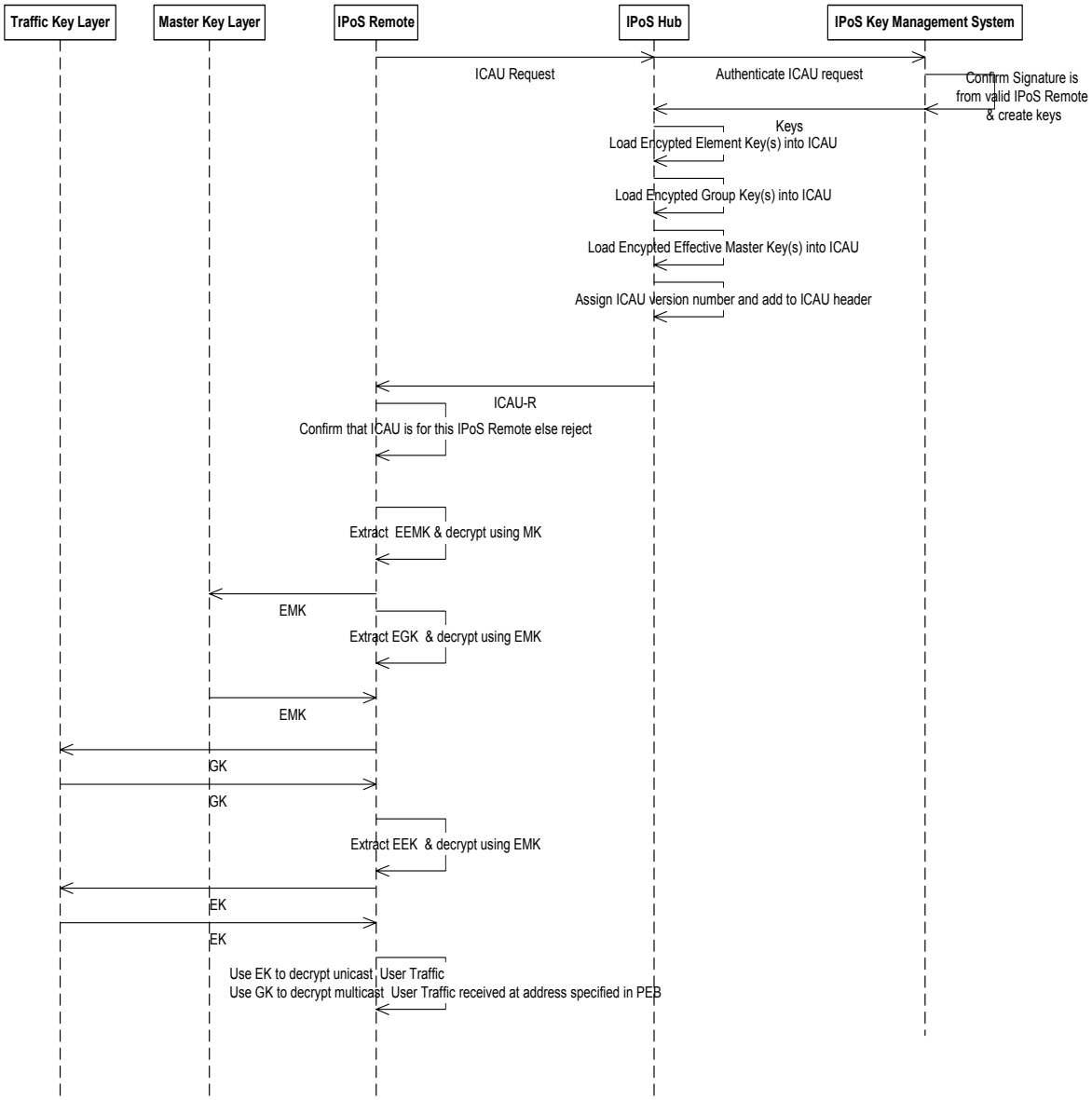


Figure B.2.5.3-1. ICAU Creation, Distribution, and Association of Keying with Layers

B.2.5.4 Periodic Element Broadcast Description

The PEB provides the IPoS remote with addressing information about each multicast group. The PEB is broadcast to the IPoS remotes on their broadcast MAC address. Only the IPoS hub can create and send a PEB. Subsection 4.13.11 defines the PEB's format.

B.2.5.5 Procedure for Initial Key Distribution During Registration and Commissioning

During commissioning of the IPoS remote, registration with the IPoS system takes place. The parameters that are required from the IPoS remote are its hardware serial number, customer name, and contact information.

From these parameters and the set of services the IPoS remote is authorized to receive, the IPoS hub can determine the set of GKs and EKs that the IPoS remote will require and the required MAC address to be used to send the keying information to the IPoS remote.

The IPoS remote will then acquire its initial keys by making an "out-of-band" ICAU Request The IPoS hub will respond to an authenticated IPoS remote's ICAU Request with an ICAU Response containing EEMK, EGKs, and EEKs for the IPoS remote.

Once a complete set of valid keys and addresses has been received by the IPoS remote, it can access IPoS services. See Figure B.2.5.5-1.

Any subsequent key updates will be made via the PACAU and PEB.

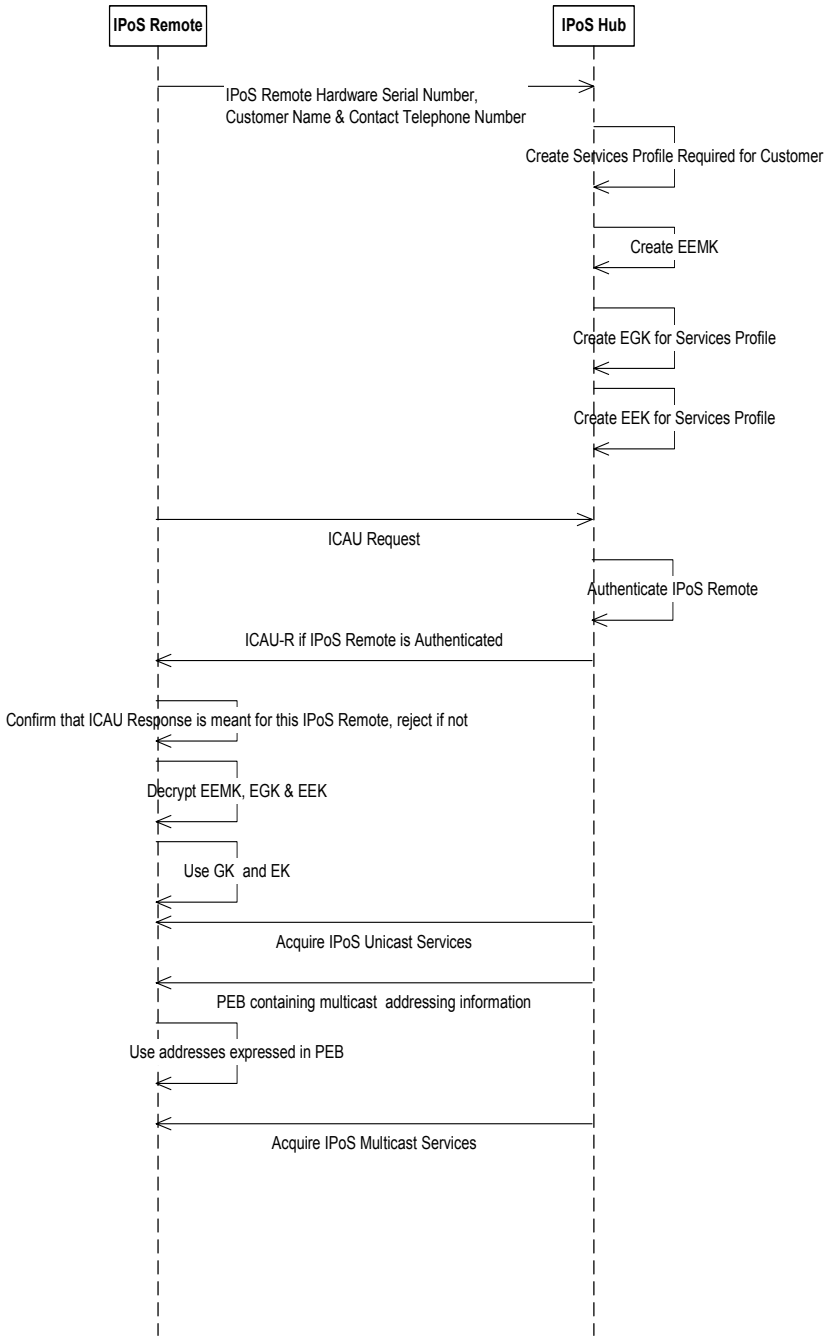


Figure B.2.5.5-1. IPoS Security-Centric View of Information Exchanges During Registration and Commissioning

B.2.5.6 Key Updates During Normal Operations

IPoS uses bulk data encryption (see reference [1], found in subsection 1.4 of this document). Additionally, the hub Key Management System can update EMKs, GKs, and EKs at any time.

IPoS uses the 2-bit payload_scrambling_control field in the outroute MAC header, with the values defined in subsection 4.10.1.2.1 to indicate whether the payload is encrypted or not.

TKs are versioned. The hub performs TK updates by distributing the next TK (with an incremented version number) ahead of time to all authorized users in order to support hitless encryption during the key update.

To update the EMK, GK and EK keys, the PACAU is used.

A key update is indicated to the IPoS remote in the PACAU. The PACAU header contains a PACAUVer field that can indicate that a key update has taken place. Every time the IPoS remote receives a PACAU, it will compare the values of the new PACAUVer field with those it has previously stored.

Should the PACAUVer field in current PACAUs be different from the PACAUVer stored by the IPoS remote, this indicates that a key update has taken place, and the IPoS remote will start to update its keys.

If the PACAU has been updated, the new versions of the keys will be embedded within the PACAU packet. Figure B.2.5.6-1 shows the update of the GKs with the PACAU.

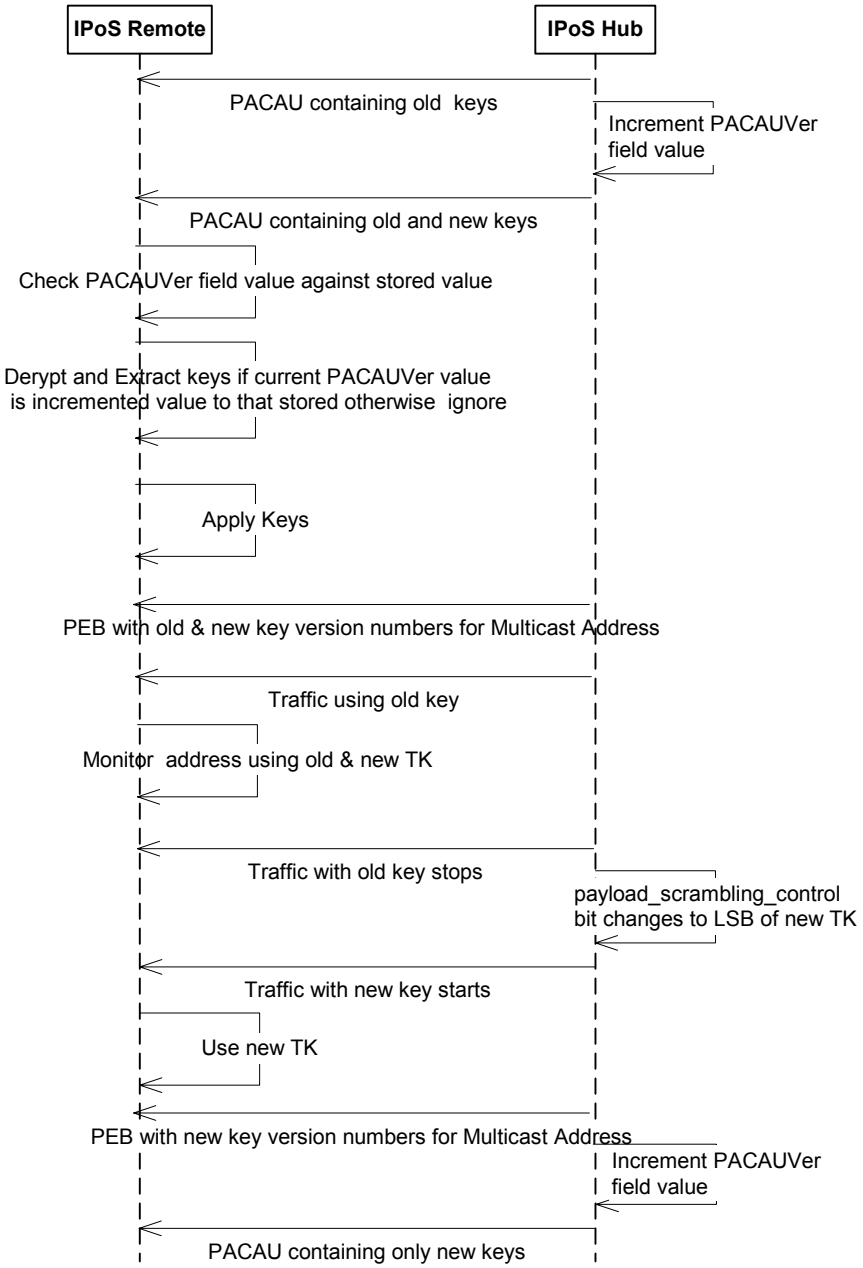


Figure B.2.5.6-1. PACAU Update Notification and Group Key Distribution Procedure

Figure B.2.5.6-2 shows the update of the EKs with the PACAU. (Note that the PEB is not required to use EKs.)

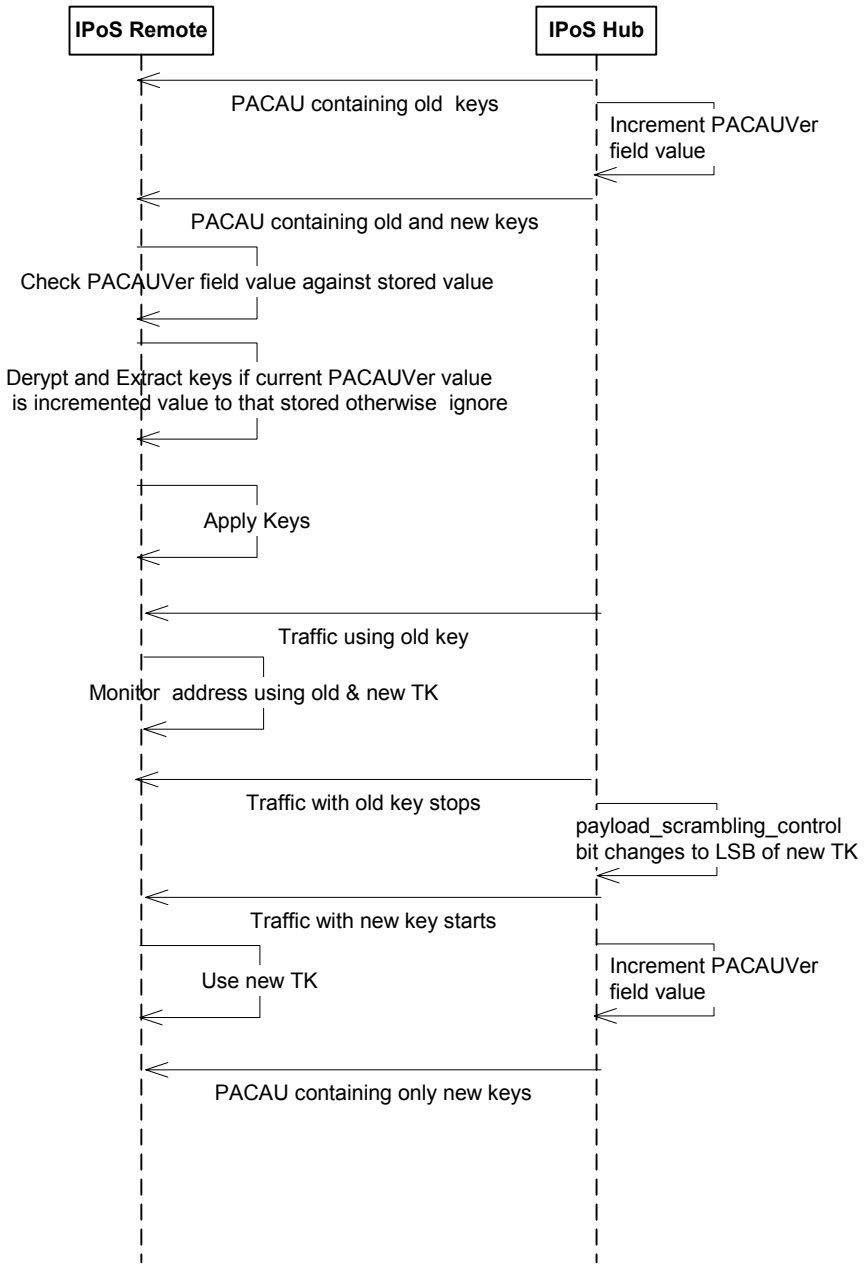


Figure B.2.5.6-2. PACAU Update Notification and Element Key Distribution Procedure

Once the IPoS remote receives EEMK, EGK, and EEK, and then successfully decrypts them, the keys are loaded into the IPoS remote's secure registry. Each key has a version number that must be preserved as a part of the key update procedure. This version number will be incremented for a new version of a TK. Additionally, a PACAU can be transmitted that has both the current and new TKs embedded within it; in this situation the IPoS remote shall continue to use the current TK and switch to the new key when commanded by the payload_scrambling_control field of the data packet.

Next, if a GK is being updated, a notification of the multicast address to which the new key applies will arrive. This notification is in the form of a PEB specifying that both the old key and new TKs are required to decrypt the multicast address for the service affected by the key update.

When the hub ceases with the old key and begins on the new key, the IPoS remote will load the new key that pertains to that multicast service and will begin to decrypt the data.

The commencement of transmission of traffic (either unicast or multicast), which is encrypted under the new TK, is indicated to the IPoS remote by placement of the new TK's version number's least significant bit (LSB) in the payload_scrambling_control field of the traffic packet.

Following the commencement of traffic using the new key, subsequent PEBs and PACAUs shall contain only the new key for the services (until another rekey is ordered).

If new EMKs are received, the IPoS remote shall immediately install and use them as required.

B.2.6 Payload Encryption/Decryption

At the beginning of each datagram to be transmitted, the IPoS hub determines the encryption key required to protect the datagram based upon the datagram's MAC address. This MAC address has previously been allocated to the datagram based upon the service to which the datagram relates.

When the datagram relates to a multicast address and requires protection, it is encrypted by the IPoS hub with the corresponding GK. The GK is a 64-bit DES key; traffic encryption in the IPoS uses single DES 64-bit encryption keys.

When the datagram relates to a unicast address and requires protection, it is encrypted by the IPoS hub with the corresponding EK. The EK is a 64-bit DES key; traffic encryption in IPoS uses single DES 64-bit encryption keys.

If the datagram does not require protection, it is not encrypted.

The EK needed at the remote terminal for decryption of the unicast datagrams is obtained by receiving the EEMK and EEK made available via the Key Distribution messages and by decrypting the EK prior to receiving the datagram.

The GK needed at the remote terminal for the decryption of the multicast datagrams is obtained by receiving the EEMK and EGK made available via the Key Distribution messages and decrypting the EGK prior to receiving the datagram.

The decryption of the EK and GK from the EEMK, EGK, and EEK uses a triple-DES algorithm and is illustrated in figure B.2.6-1.

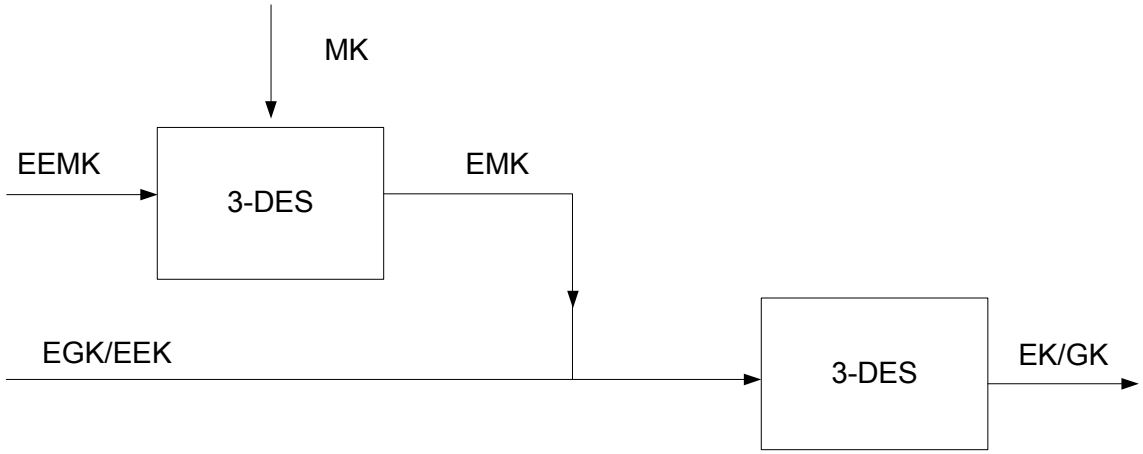


Figure B.2.6-1. Decryption of EK and GK Keys

The MAC address to which the encrypted multicast user data packets will be transmitted to the IPoS remote has been made available via PEB messages (described in subsection B.2.5) prior to receiving the datagram.

The header of each datagram is left unencrypted so that the IPoS remote can read the MAC addressing information.

Triple-DES decryption of the encrypted payload of each received packet is performed at the remote terminal according to the following steps:

1. Upon reception at the IPoS remote, the remote can use the datagram's destination MAC address. The MAC address to GK mapping information is provided in the PEB packet, and the GK is to be used to decrypt the datagram.

2. An EK is identified by an Element_ID (in a PACAU) or Group_ID (in a ICAU-R) field value 0x0000FF.

3. The content of each datagram section contains the 8-byte initialization vector (see subsection 4.10.1.2.2) to the Cipher Block Chaining (CBC) DES decryption mode used in IPoS.

4. Once the remote terminals have selected the appropriate decryption key, the key is loaded into the appropriate register of the DES decryption element.

5. The payload of the received packet is loaded into the input register.

6. Unencrypted data is provided by the DES decryptor into the output register.

TIA